
**Universidad Nacional Mayor de San Marcos**

**Universidad del Perú. Decana de América**

Facultad de Ingeniería de Sistemas e Informática

Escuela Académico Profesional de Ingeniería de Sistemas


# Implementación de un sistema de control de acceso para mejorar la seguridad de la información de la empresa SNX S.A.C.

**TESINA**

Para optar el Título Profesional de Ingeniero de Sistemas


**AUTOR**

Miguel Alejandro Martín RIVAS ARELLANO

**ASESOR**

Frank Edmundo ESCOBEDO BAILÓN



Lima, Perú

2016

Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

https://creativecommons.org/licenses/by-nc-sa/4.0/

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

**Referencia bibliográfica**

Rivas, M. (2016). *Implementación de un sistema de control de acceso para mejorar la seguridad de la información de la empresa SNX S.A.C.* [Tesina de pregrado, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática, Escuela Académico Profesional de Ingeniería de Sistemas]. Repositorio institucional Cybertesis UNMSM.

**UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS**
**FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMATICA**
**PROGRAMA DE ACTUALIZACIÓN PROFESIONAL 2014-II**

# Acta de Sustentación de Tesina

Siendo las 20:40 del día 13 de Mayo del año 2016, se reunieron los docentes designados como miembros de Jurado de la Tesina, presidido por el Ing. Carlos Ernesto Chávez Herrera, el Msc. Juan Gamarra Moreno, (Miembro) y el Dr. Frank Edmundo, Escobedo Bailón (Miembro Asesor) para la sustentación de la Tesina intitulada: "IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA SNX S.A.C". Por el Sr. Bach, MIGUEL ALEJANDRO MARTÍN RIVAS ARELLANO; para optar el Título Profesional de Ingeniero de Sistemas.

Acto seguido de la exposición de la Tesina, el Presidente invitó al graduando a dar respuesta a las preguntas establecidas por los Miembros de Jurado.

El graduando en el curso de sus intervenciones demostró pleno dominio del tema, al responder con acierto y fluidez a las observaciones y preguntas formuladas por los señores miembros del Jurado.

Finalmente habiéndose efectuado la calificación correspondiente por los miembros de Jurado, el graduando obtuvo la nota de 17 (En letras) Diecisiete

A continuación el Presidente del Jurado el Ing. Carlos Ernesto, Chávez Herrera declara al graduando **Ingeniero de Sistemas.**

Siendo las 21:45 horas, se levantó la sesión.

.....
Presidente
Ing. Carlos Ernesto, Chávez Herrera

.....
Miembro
Msc. Juan Gamarra Moreno

.....
Miembro Asesor
Dr. Frank Edmundo, Escobedo Bailón

FICHA CATALOGRÁFICA

RIVAS ARELLANO, Miguel Alejandro Martín

IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA SNX S.A.C.

SEGURIDAD DE LA INFORMACIÓN
(Lima, Perú 2016)

Tesina, Facultad de Ingeniería de Sistemas e Informática, Pregrado, Universidad Nacional Mayor de San Marcos

**DEDICATORIA**

Dedico este trabajo de tesina primeramente a Dios, por darme la perseverancia suficiente para poder hacer frente a las dificultades presentes en el día a día; a mis padres, por el constante apoyo que me brindan y los sabios consejos que siempre me imparten; y a todos aquellos que de una u otra manera me brindaron su apoyo para poder alcanzar mis objetivos profesionales; siempre estarán presentes.

## AGRADECIMIENTOS

Al profesor Dr. Frank Edmundo Escobedo Bailón, por su excelente dedicación y apoyo incondicional durante el desarrollo de la presente tesis.

A los docentes en general, quienes me brindaron su asesoramiento durante toda mi experiencia universitaria.

A mis amigos y colegas de trabajo; quienes me aconsejaron y facilitaron el acceso a toda la información necesaria para el desarrollo del presente trabajo.

# UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

## FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

### ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS


# IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO PARA MEJORAR LA SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA SNX S.A.C.


Autor: RIVAS ARELLANO, Miguel Alejandro Martín.

Asesor: Dr. ESCOBEDO BAILÓN, Frank Edmundo.



Título: Tesina para optar el Título Profesional de Ingeniero de Sistemas.

Fecha: Mayo 2016.


---

## RESUMEN


La información hoy en día representa un activo valioso para las organizaciones, por ende esta mayormente digitaliza y almacenada en sistemas informáticos que puedan brindar una alta disponibilidad e integridad a ella. Es por ello que, proporcionar un acceso adecuado a estos sistemas de información debería ser uno de los puntos más relevantes que deben de tomar en cuenta las organizaciones, con el fin de mejorar sus procesos de seguridad de la información. En este trabajo se propone la implementación de un sistema de control de acceso que pueda ser integrado al sistema de servidores de archivos donde es almacenada la información de la empresa SNX S.A.C., y de esa manera poder mejorar sus procesos de seguridad de la información.



***Palabras claves:*** *Control de acceso, sistema de control de acceso, seguridad de a información, sistema de gestión de la seguridad de la información, tecnologías de la información.*

# UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS

## FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

### ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS


# IMPLEMENTATION OF AN ACCESS CONTROL SYSTEM TO IMPROVE INFORMATION SECURITY OF THE ENTERPRISE SNX S.A.C.


Autor: RIVAS ARELLANO, Miguel Alejandro Martín.

Asesor: Dr. ESCOBEDO BAILÓN, Frank Edmundo.



Título: Tesina para optar el Título Profesional de Ingeniero de Sistemas.

Fecha: Mayo 2016.


---

## ABSTRACT


Today, the information represents a valuable asset for organizations, therefore is mostly digitized and stored in computer systems that can provide high availability and integrity to it. It is for them that, to provide adequate access to these information systems should be one of the most important points that must be taking into account by the organizations, in order to improve their processes of information security. In this paper we propouse the implementation of an access control system that can be integrated into the system of file servers where is stored the information of SNX S.A.C. company, and thus to improve their processes information security.



***Key words:*** *Access control, access control system, information security, informations security management system, information technologies.*

# ÍNDICE DE CONTENIDOS

# ÍNDICE DE FIGURAS

# CAPÍTULO I. PLANTEAMIENTO METODOLÓGICO

## 1. Antecedentes del problema

A continuación, se presentara los artículos científicos relacionados a nuestro caso de estudio y que fueron revisados para poder determinar a los antecedentes de nuestro problema a tratar en el presente trabajo:

- En *Access control for rural medical and health collaborative working platform* (Yang-Feng et al., 2013, p.07) se narra sobre la necesidad de los datos privados de los usuarios de contar con una fuerte protección de la seguridad dentro de una plataforma de trabajo colaborativo. Ante ello, los autores plantearon un análisis sobre el control de acceso y su implementación dentro en una plataforma de trabajo colaborativo, desde la perspectiva de la gestión de roles de usuarios. Se tomo como caso de estudio a la plataforma de trabajo colaborativo para la salud y medicina rural, perteneciente al proyecto de medicina básica rural e investigación médica del Ministerio de Ciencia y Tecnología de China. Los autores concluyeron que la implementación de un control de acceso en la plataforma asegura que los datos pueden ser almacenados de forma segura y confidencial, ademas de proteger la seguridad de los datos compartidos entre los pacientes y los médicos permitiendo el acceso de los usuarios al sistema en un rango controlado. Finalmente, el aporte realizado en la investigación fue dotación de usuarios con diferentes permisos, acorde a los diferentes roles de usuario presentes en cada uno de los cuatro módulos de la plataforma de trabajo colaborativo.

- En *An access control model for cloud computing* (Tounis, Kifayat y Merabti, 2014, p.45) se narra sobre los problemas asociados a la utilización de la computación en la nube, tales como la seguridad de los datos, el abuso de los servicios en la nube, la presencia de usuarios maliciosos y ataques cibernéticos, así como las limitación que tienen los modelos de control de acceso tradicionales para cumplir con los requisitos de control de acceso de la nube. Ante ello, los autores plantearon un análisis detallado de los requisitos de control de acceso para la computación en la nube y la identificación de los vacíos relevantes que no son cumplidos por los modelos convencionales. Así también se propone un modelo de control de acceso que pueda cumplir con estos requisitos identificados. Se tomo como caso de estudio su

implementación en un sistema que utiliza los tres servicios diferentes que ofrece la computación en la nube (como *SaaS*, *PaaS* e *IaaS*) y que fue implementados sobre la infraestructura de un proveedor de servicios en la nube. Los autores concluyeron que el modelo propuesto facilita los principios de roles y tareas para hacer muy dinámico y fácil la asignación de privilegios. Finalmente, el aporte realizado en la investigación fue la utilización de un motor de riesgo para hacer frente a los comportamientos dinámicos y aleatorios de los usuarios, y la utilización de un motor de etiquetas de seguridad para la emisión y marcado de los datos con etiquetas que demuestren la sensibilidad de los datos, en entornos y procesos parcialmente confiables o no confiables.

- En *An enhancement of the Role-based access control model to facilitate information access management in context of team collaboration and workflow* (Hung, Doll, Barbosu, Luque y Wang, 2012, p.1084) se narra sobre la limitada capacidad que tienen los modelos de control de acceso a la información cuando se trata de implementarlos en un contexto de colaboración y trabajo en equipo. Ante ello, los autores plantearon realizar una mejora al modelo de control de acceso basado en roles. Se tomo como caso de estudio su implementación dentro del proyecto de "*Iniciativa de educación clínica HIV*" del estado de New York, en donde se ilustran los conceptos del modelo mejorado. Los autores concluyeron que el modelo de control de acceso mejorado puede ser utilizado con eficacia para administrar el acceso a la información en los procesos de colaboración para la coordinación de un programa de educación clínica. Finalmente, el aporte realizado en la investigación fue formulación de las limitaciones generales, la definición clara de las entidades y atributos, la extensión de permisos de acceso para incluir el contexto de flujo de trabajo en equipo y el desarrollo de ontologias del dominio como ejemplificaciones del modelo general, para las aplicaciones especificas.

- En *An extended attribute based access control model with trust and privacy: Application to a collaborative crisis management system* (Smari, Clemente y Lalande, 2014, p.147) se narra sobre las carencias que posee el modelo básico de control de acceso basado en atributos para tratar los aspectos de contexto, confianza y privacidad en entornos de colaboración distribuidos de alto rendimiento. Ante ello, los autores plantearon un modelo

de control de acceso extendido basado en atributos, asociándolos a objetos y sujetos, ademas de que incorpore los aspectos de confianza y privacidad con el fin de tomar decisiones de control de acceso sensibles al contexto de colaboración entre organizaciones. Se tomo como caso de estudio su implementación en una plataforma de gestión de crisis ante desastres naturales, el cual permite que los militares, policías, bomberos, agentes federales, personal médico, y la gente común pueda colaborar para el rescate de personas. Los autores concluyeron que el modelo propuesto es especialmente útil para entornos de colaboración altamente dinámicos y plantea una forma idílica para la escritura de políticas de seguridad para cada uno de los tipos de entornos de colaboración. Finalmente, el aporte realizado en la investigación fue la utilización de una función que calcula la confianza requerida de cada sujeto solicitante con respecto a los atributos de los objetos accedidos y la utilización de un motor de decisión que evalúa las solicitudes de lectura de atributos y las solicitudes de actualización recibidas de otros usuarios.

- En *domRBAC: An access control model for modern collaborative systems* (Gouglidis y Mavridis, 2012, p.540) se narra sobre la necesidad de contar con la capacidad de poder usar fuertes restricciones sobre los recursos y de manejar políticas de seguridad en un manera fácil y eficiente dentro de organizaciones virtuales. Ante ello, los autores plantearon un modelo de control de acceso mejorado basado en roles, el cual titulan como *domRBAC*. Se tomo como caso de estudio su implementación en un simulador capaz de adoptar las definiciones del mismo modelo de control de acceso y en donde se llevaron a cabo los estudios experimentales. Los autores concluyeron que el modelo propuesto es capaz de ejecutar las políticas de seguridad entre varios dominios, contando cada uno con políticas de seguridad diferentes, ademas de garantizar un entorno de colaboración seguro mediante la graduación y revisión constante de las violaciones de las políticas, que pueden ser causadas por una nueva asignación de roles entre dominios. Finalmente, el aporte realizado en la investigación fue la elaboración del modelo *domRBAC* basándose en la adaptación modelo de control de acceso *ANSI INCITS 359-2004*; el cual es capaz de diferenciar las políticas de seguridad que se deban cumplir en cada organización.

- En *Extended access control and recommendation methods for enterprise knowledge management system* (Wang, Guo, Fan y Bi, 2014, p.224) se narra sobre las deficiencias que existen en los métodos tradicionales de control de acceso cuando son implementados en los sistema de gestión del conocimiento de gran tamaño. Ante ello, los autores proponen un modelo extendido de control de acceso basado en roles para superar tales deficiencias; ademas de una colección de recomendaciones híbridas para los sistemas de gestión del conocimiento. Se tomo como caso de estudio su implementación dentro de un sistema empresarial de gestión del conocimiento que cuente con varios departamentos y organizaciones virtuales. Los autores concluyeron que el modelo propuesto, que ademas conserva muchas de las principales características del modelo de control de acceso basado en roles, hace más fácil la administración del control de acceso cuando es implementado en un sistema empresarial de gran tamaño. Finalmente, el aporte realizado en la investigación fue la introducción de una estructura de grupos de usuarios en dos tipos, a los cuales se le puedan añadir los usuarios, los privilegios y roles.

- En *Privacy aware access control for big data: A research roadmap* (Colombo y Ferrari, 2015, p.01) se narra sobre los inadecuados mecanismos de protección de datos lo cual impide la adopción del paradigma de *Big Data* en varias compañías. Ante ello, los autores proponen un plan de investigación y desarrollo de un marco de trabajo que apoye a la integración de funciones de control de acceso conscientes de la privacidad, en las plataformas de *Big Data*. Se tomo como caso de estudio la implementación del marco de trabajo dentro de sistemas de *Big Data* tales como sistemas *MapReduce* y bases de datos *NoSQL*. Los autores concluyeron que con el fin de mostrar la aplicación del marco de trabajo propuesto, se deben de proporcionar algunas consideraciones relacionadas con el mejoramiento de algunas plataformas de *Big Data*. Finalmente, el aporte realizado en la investigación fue la creación de una hoja de ruta para el desarrollo del marco de trabajo, la cual abarca variedad de actividades, tales como la selección de las plataformas destino, la identificación de las políticas adecuadas para los escenarios de aplicación común de las plataformas de *Big Data* y la definición de especificaciones de las políticas y mecanismo de aplicación.

- En *Relation Based Access Control in Campus Social Network System* (Du, Lie y Wang, 2013, p.14) se narra sobre la necesidad de integrar el control de acceso a un sistema de red social de campus para que se ocupe del acceso a la información y a los recursos relacionados con el espacio personal de cada usuario y los espacios compartidos entre grupos de usuarios. Ante ello, los autores proponen el diseño de un modelo de control de acceso basado en relaciones el cual pueda asignar permisos en base a las relaciones sobre la información y recursos que los usuarios dispongan. Se tomo como caso de estudio su implementación dentro del sistema de red social de campus de la universidad de ciencias y tecnología de Beijing. Los autores concluyeron que el modelo es desarrollado por una inteligencia colectiva, reflejada a través de la identidad de sus usuarios, sus relaciones sociales y los permisos que establecen sobre los perfiles de usuario y el contenido creado por ellos. Finalmente, el aporte realizado en la investigación fue la construcción del sistema basándose en el modelo relacional del sistema, teniendo una composición en base a ocho elementos básicos: usuarios, grupos, relaciones usuario – usuario, relaciones usuario – grupo, operaciones, información, recursos y permisos.

- En *Role-based access control for substation automation systems using XACML* (Lee, Kim, Yang y Jang, 2015, p.237) se narra sobre la creciente necesidad de acceder a los datos de los equipos internos y dispositivos de un sistema de subestación desde sistemas externos y la creciente preocupación sobre la seguridad de los datos. Ante ello, los autores plantean un nuevo enfoque para la implementación de un modelo de control de acceso basado en roles, siguiendo las especificaciones de la norma *IEC 62351* y utilizando *XACML*, como lenguaje estándar para la descripción de las políticas de control de acceso. Se tomo como caso de estudio su implementación dentro de los sistemas de automatización de subestaciones, pertenecientes a una red eléctrica avanzada . Los autores concluyeron que el enfoque que se presenta es flexible para dar cabida a futuras ampliaciones y que como el sistema de subestación es estable en términos de los elementos del modelo de control de acceso basado en roles, se espera que los cambios futuros en las políticas de acceso tengan un impacto mínimo en el entorno de producción. Finalmente, el aporte realizado en la investigación fue la implementación del sistema de control de acceso usando las librerías de código abierto OpenIE61850 para los servicios de comunicación abstracta.

## 2. Definición del problema

A partir del análisis realizado por cada uno de los escenarios presentes en los artículos de investigación, hemos podido identificar los siguientes inconvenientes:

- La necesidad de integrar un control de acceso para que se ocupe del acceso a la información y a los recursos relacionados con el espacio personal de cada usuario y los espacios compartidos.
- La necesidad de contar con una fuerte protección de la seguridad para los datos privados de los usuarios y evitar el abuso de los servicios disponibles, la presencia de usuarios maliciosos y otros ataques cibernéticos.
- La necesidad de contar con la capacidad de usar fuertes restricciones sobre los recursos y de manejar políticas de seguridad en un manera fácil y eficiente.
- La creciente necesidad de acceder a los datos de los equipos internos y dispositivos.

Es por eso que se puede determinar que el principal problema asociado a estos escenarios es que cuentan con la presencia de procesos inadecuados de seguridad de la información en los sistemas informáticos que emplean, específicamente a los procesos relacionados con el control de acceso a la información.

Brindar un control de acceso adecuado es un requisito esencial en cualquier entorno, ya que facilitar y proteger el acceso de los usuarios hacia los sistemas de información es un enfoque eficaz para hacer frente a las necesidades de información, mejora la colaboración y el trabajo en la organización. También, debido a que los requisitos de acceso a la información están cambiando constantemente, se requiere contar con un manejo ágil del nivel de acceso, con el fin de que los requerimientos de acceso a la información se adapten más rápido a un contexto específico de trabajo o en su defecto a algún requisito en particular del equipo que requiera contar con la información.

# 3. Objetivos

## *3.1. Objetivo General*

El objetivo del presente trabajo es implementar un sistema de control de acceso para mejorar la seguridad de la información en la empresa SNX S.A.C, y que a su vez pueda garantizar la confidencialidad, integridad y disponibilidad de su información a los usuarios de la organización.

## *3.2. Objetivos Específicos*

A continuación pasaremos a describir algunos objetivos específicos que buscamos concretar, con forme se vaya desarrollando el presente trabajo:

- Realizar un análisis detallado sobre los modelos de control de acceso existentes para poder seleccionar el más adecuado en relación a nuestro escenario.
- Realizar un análisis detallado sobre las herramientas existentes en el mercado que tengan las capacidades de poder brindar un control de acceso hacia otros sistemas informáticos.
- Definir los componentes que se utilizaran, de acuerdo al modelo de control de acceso seleccionado y el escenario en donde se desarrollara este proyecto.
- Definir las políticas de control de acceso en relación a las funciones que desempeñas los actores en la organización.
- Configuración de la herramienta seleccionada como un sistema de control de acceso, en base a las especificaciones del modelo de control de acceso generado.
- Integrar el sistema de control de acceso a la granja de servidores alojados en la empresa.

## 4. Alcance del estudio

A continuación pasaremos a describir los alcances o limitaciones que tomaremos en cuenta para el desarrollo del presente trabajo:

- El campo de estudio sobre el cual se desarrollara este trabajo es sobre el campo de la seguridad de la información.
- Dentro del campo de estudio de la seguridad de la información, hemos optado por solo tomar en cuenta lo referente al dominio del control de acceso.
- Dentro del dominio del control de acceso, solo pretendemos hacer uso de controles del tipo lógico, de toda la gama de tipos de controles disponibles en el domino.
- Solo se controlara el acceso a información ya computarizada y almacenada dentro del sistema de servidores de archivos disponibles en la empresa.
- El escenario sobre el cual se desarrolla este trabajo es dentro de la empresa regional de servicios de TI SNX S.A.C., que cuenta con presencia en Perú, Chile y Argentina.
- Dentro de la empresa, solo tomaremos en cuenta la sede ubicada en Lima, Perú, dejando de lado las necesidades de información que tienen las demás sedes.
- Dentro de la gama de servicios de TI que ofrece la empresa, solo se considerada controlar el acceso a la información generada por su servicio de "Gestión de proyectos y consultoría".
- Finalmente el sistema de control de acceso solo interactuara a lo más con los sistemas de controlador de domino y servidores de archivos de la organización. Los cuales se encuentran desplegados sobre *Windows Server 2008 R2* y R*ed Hat Enterprise Linux* con la aplicación *Samba* respectivamente.

## 5. Organización de la tesina

El presente trabajo se encuentra organizado por cinco capítulos, los cuales pasaremos a describir a continuación:

- En el capítulo I se realizara el planteamiento metodológico, él cual abarcara inicialmente a los antecedentes y la descripción del problema a tratar, los objetivos que se buscan alcanzar, la justificación y la delimitación del alcance para la solución propuesta.
- En el capitulo II se realizara el estudio del marco teórico, el cual incluirá a los principales conceptos sobre el control de acceso, sus modelos o técnicas y conceptos sobre la seguridad de la información.
- En el capítulo III se realizara el estudio del estado del arte, el cual abarcara un estudio sobre los modelos de control de acceso más relevantes, las tecnologías de información en el mercado que puedan cumplir con las funciones de un sistema de control de acceso y los casos de estudio en donde se hayan encontrado una solución a problemas similares al nuestro.
- En el capítulo IV se realizara el diseño y la implementación de nuestra solución propuesta, abarcando primero la adecuación del modelo de control de acceso seleccionado a nuestro escenario y concluirá con el despliegue del sistema de información tomando en cuentas la estructura y las políticas previamente establecidas en el modelo.
- En el capítulo V se realizara finalmente las conclusiones del presente trabajo y las recomendaciones que pudieran servir para la elaboración de trabajos futuros.

# CAPÍTULO II. MARCO TEÓRICO

## 1. Control de acceso

### *1.1. Definición*

Peltier (2014) define que el control de acceso se trata sobre los sistemas que protegen a los objetos de valor y también sobre las decisiones tomadas por las personas que determinan quien recibe alguna clase de acceso. El control de acceso puede ser utilizado para controlar el acceso a espacios físicos o a la información dentro de un sistema (p.204).

## 2. Sistema de control de acceso

### *2.1. Definición*

Peltier (2014) define que los sistemas de control de acceso se ponen en marcha para garantizar que sólo las personas autorizadas tengan acceso a la información, y que para que la información se mantenga intacta y disponible cuando sea necesario. El propósito de los sistemas de control de acceso es evitar la modificación de la información por los usuarios no autorizados, permitir la modificación de la información por los usuarios autorizados, y preservar la consistencia interna y externa de los datos. (p.205).

Para lograr esto, se aplican los controles. Los controles ayudan a mitigar el riesgo y reducir la posibilidad de pérdida, y requiere de las combinaciones de controles para una defensa en profundidad. Una forma de clasificar a los controles de acceso es mediante la descripción en la forma en que se implementan. Los tres tipos diferentes de implementación son: administrativos, físicos y técnico / lógicos. (Peltier, 2014, p.206).

### *2.2. Tipos de controles*

- **Controles administrativos**

  Los controles administrativos ayudan a hacer frente a las amenazas internas, como el robo de información privilegiada o violación a bases de datos. Estos controles

pueden ser las políticas, procedimientos, capacitaciones, revisiones, etc, que establece la organización.. (Peltier, 2014, p.206).

- **Controles físicos**

  Los controles físicos se utilizan para disuadir y prevenir eventos desastrosos dentro de un ambiente físico, puede ser tales como guardias de seguridad, cámaras de seguridad, asegurando de salas de servidores, el bloqueo de los ordenadores portátiles, etc. (Peltier, 2014, p.206).

- **Controles técnicos o lógicos**

  Los controles técnicos o lógicos restringen el acceso a los sistemas de información y protegen la información que ellos contienen; tales como el cifrado, tarjetas inteligentes, listas de control de acceso, protocolos de transmisión, etc. (Peltier, 2014, p.207).

## 3. Seguridad de la información

### *3.1. Definición*

La seguridad de la información protege a la información de un amplio rango de amenaza para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retornos de las inversiones y oportunidades del negocio, preservando la confidencialidad, integridad y disponibilidad de la información, así mismo, otras propiedades como la autenticidad, no rechazo, contabilidad y confiabilidad también pueden ser consideradas. ("Norma Técnica Peruana", 2007, p.08).

### *3.2. Características*

- **Confidencialidad**

  La confidencialidad es la propiedad de garantizar que la información sea accesible únicamente para quienes tengan acceso autorizado. ("Norma Técnica Peruana", 2009, p.11).

- **Integridad**

  La integridad se define como la propiedad de salvaguardar con exactitud e integridad de la información y los activos asociados a él. ("Norma Técnica Peruana", 2009, p.11).

- **Disponibilidad**

  La disponibilidad se define como la propiedad de garantizar que los usuarios autorizados tengan acceso a la información y activos asociados cuando sea necesario. ("Norma Técnica Peruana", 2009, p.12).

## 4. Sistema de gestión de la seguridad de la información

### *4.1. Definición*

El sistema de gestión de la seguridad de la información es la parte del sistema integral de gestión, basado en un enfoque del riesgo del negocio para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información. Una organización deberá desarrollar, implementar, operar, monitorizar, revisar, mantener y mejorar continuamente un SGSI documentado dentro del contexto de las actividades y riesgos totales de la organización. El proceso usado para su desarrollo se basa en el modelo *PDCA* o también llamado *Ciclo de Deming*. ("Norma Técnica Peruana", 2009, p.13).

### *4.2. Ciclo de Demming*

El ciclo de Deming que también es conocido como el modelo *Plan-Do-Check-Act* y puede aplicar para el desarrollo de un sistema de gestión de la seguridad de la información bajo un enfoque de procesos. ("Norma Técnica Peruana", 2009, p.06). Esta compuesto por las siguientes tareas:

- **Proceso Plan**

  El proceso *Plan* o *Planificar* se encarga de establecer las políticas, objetivos, procesos y procedimientos de seguridad relevantes para administrar el riesgo y mejorar la seguridad de la información para obtener resultados de acuerdo con las políticas y objetivos de la organización. ("Norma Técnica Peruana", 2009, p.07).

- **Proceso Do**

  El proceso *Do* o *Hacer* se encarga de implementar y operar las políticas, controles, procesos y procedimientos de seguridad. ("Norma Técnica Peruana", 2009, p.07).

- **Proceso Check**

  El proceso *Check* o *Verificar* se encarga monitorizar y evaluar el funcionamiento de los procesos con respecto a las políticas, objetivos y experiencia práctica de seguridad, informando sobre los resultados obtenidos a la gerencia para su revisión. ("Norma Técnica Peruana", 2009, p.07).

- **Proceso Act**

  El proceso *Act* o *Actuar* se encarga de tomar las acciones correctivas y preventivas basándose en los resultados de la revisión general para alcanzar la mejora continua del SGSI. ("Norma Técnica Peruana", 2009, p.07).

## 5. Conceptos complementarios

### *5.1. Gestión de acceso a los usuarios*

Peltier (2014) define que la gestión de acceso a los usuarios trata de asegurar que los usuarios autorizados tengan un acceso adecuado al sistema y evitar el acceso no autorizado al sistema. La ISO 27002 describe varias áreas donde la gestión de acceso a los usuarios debe ser considerado. Estas áreas incluyen: *registro del usuario*, *gestión de privilegios*, *administración de contraseñas de usuario* y *revisión de los derechos de acceso de los usuarios*. (p.208).

- **Registro de usuarios**

  El registro de usuarios también se conoce como la autorización de la cuenta de usuario es una de las piezas más importantes del proceso de acceso. Es la forma en que los usuarios establecen el acceso al sistema y también determina el acceso que el usuario tendrá una vez dentro del sistema. Es necesario contar con un proceso formal el cual debe incluir la aprobación de la parte autorizada para que el usuario obtenga acceso, y el usuario deberá estar obligado a firmar un acuerdo de usuario que indique que entiendan sus responsabilidades por el uso de la cuenta. Todos los ID de usuario deben ser únicos y cada usuario puede tener uno y sólo un ID de usuario para cada sistema. La documentación relativa a la creación de una cuenta de usuario y el acceso otorgado a la cuenta debe mantenerse siempre y cuando el usuario es un empleado activo en el mismo departamento. Así como el registro de usuarios y de los procesos que lo rodean son importantes, también lo son los procesos implementados para la eliminación de la cuenta de usuario, o cancelación del registro. Estos procesos deben documentarse y conocerse. (Peltier, 2014, p.209).

- **Gestión de privilegios**

  La gestión de privilegios ajusta los privilegios de usuarios con respecto al cambio de responsabilidades dentro del trabajo. Es común para que una empresa de querer otorgar altos niveles de acceso a un usuario que está muy bien informado acerca de

un sistema, pensando que la persona puede entonces ser más servicial y más productivo. La gestión de privilegios considera el principio de privilegios mínimos necesarios que deben de aplicarse a los sistemas a la hora de conceder acceso de los usuarios, para que una persona pueda llevar a cabo sus funciones de trabajo. Siempre que sea posible, un empleado de comenzar un nuevo trabajo debe ser relevado de sus antiguas responsabilidades de trabajo y el acceso a las anteriores responsabilidades requeridas. Tener una copia de seguridad para puestos críticos hace que este proceso sea mucho más eficiente. (Peltier, 2014, p.209).

- **Administración de contraseñas de usuarios**

  La administración de contraseñas de usuarios debe hacer cumplir que las contraseñas sean seguras en los sistemas, ya que mientras más fuerte sea la contraseña, más difícil será de descifrar. Hay muchas directrices para seleccionar contraseñas seguras. El estado más común es que deben tener al menos ocho caracteres de longitud, que no se base en palabras de diccionario, y que debe contener una combinación de letras mayúsculas y minúsculas, números y caracteres especiales. Existen incluso consejos para hacer contraseñas fáciles de recordar, una técnica para crear una contraseña fácil de recordar es usar una frase de paso. (Peltier, 2014, p.210).

- **Revisión de los derechos de acceso de los usuarios**

  La revisión de los derechos de acceso de los usuarios hace recordar que el control de acceso también es importante en el entorno físico. Políticas tales como de escritorio limpio pretenden que los usuarios sepan que es su responsabilidad asegurarse de que cuando están lejos de su escritorio, todos los papeles sensibles deben estar encerrados y que se debe de usar un protector de pantalla protegido con contraseña para que nadie pueda acceder a un sistema en que se registren. Las políticas también pueden ser una buena manera de asegurarse de que los usuarios protejan sus ordenadores portátiles con un cable de seguridad cuando están lejos y no tienen su ordenador portátil con ellos. La información sensible almacenada en medios extraíbles se debe exigir a cifrar. (Peltier, 2014, p.212).

### *5.2. Protocolos de red*

- **Domain Name System**

  *Domain Name System* o *DNS* es un sistema de nombres jerárquico y distribuido para la gestión de la asignación de nombres entre dominios, hosts y servidores con direcciones *IP*. *DNS* también define el protocolo para el intercambio de comunicaciones *DNS* como parte de la suite de protocolos de Internet o *IP*. (Helsin, 2013, p.07).

- **Network Time Protocol**

  *Network Time Protocol* o *NTP* es un protocolo de *Internet* que se utiliza para sincronizar los relojes de los computadores personales o servidores con una fuente referencial de tiempo. (Helsin, 2013, p.07).

- **Name Service Switch**

  *Name Service Switch* o *NSS* permite que la información de los usuarios y del sistema (contraseña, grupos, nombre de host, etc.) sean obtenidas desde diferentes servicios con bases de datos tales como *DNS*, *LDAP*, *NIS* o archivos locales. (Helsin, 2013, p.07).

- **Kerberos**

  *Kerberos* es un protocolo de autenticación de red que utiliza la criptografía de clave simétrica para proporcionar una autenticación altamente segura entre los cliente y el servidor de aplicaciones. Kerberos opera sobre la base de "tickets" que se conceden por un tercero llamado centro de distribución de claves o *KDC*. El *KDC* mantiene una base de datos segura de claves secretas que son conocidas sólo por el propio *KDC* y el cliente que solicita un ticket. La autenticación por *Kerberos* es significativamente más segura que la autenticación basada en contraseñas, porque las contraseñas no se envían por la red - incluso cuando se accede a los servicios en otras máquinas. (Helsin, 2013, p.06).

- **Lightweight Directory Access Protocol**

  *Lightweight Directory Access Protocol* o *LDAP* es un conjunto de protocolos abiertos que se utilizan para acceder a la información almacenada dentro de una red. Se basa en el estándar *X.500* para compartir directorios, pero es menos complejo y consume muchos menos recursos. *LDAP* organiza la información de manera jerárquica, basándose en el uso de directorios, estos directorios pueden almacenar una gran variedad de información y se pueden usar de forma similar al servicio de información en red o *NIS*, permitiendo que cualquiera pueda acceder a su cuenta desde cualquier máquina en la red. Actualmente, *LDAP* se usa más dentro de organizaciones individuales, como universidades, departamentos gubernamentales y empresas privadas. El servidor de *LDAP* puede usar una variedad de bases de datos para guardar los directorios, cada uno optimizado para operaciones de lectura rápidas y reiterativas. La principal ventaja de *LDAP* es que la información de toda una organización se puede consolidar en un repositorio central. (Helsin, 2013, p.06).

- **Server Message Block/Common Internet File System**

  *Server Message Block* o *SMB* es igual a *Common Internet File System* o *CIFS* y es un protocolo de red desarrollado para facilitar las comunicaciones entre clientes y servidores para los servicios de archivos e impresión. El protocolo *SMB* fue desarrollado originalmente por *IBM* y posteriormente ampliado por *Microsoft* con el nombre de protocolo *CIFS*. Los términos *SMB* y *CIFS* son a menudo intercambiables, pero desde una perspectiva funcional, ambos son protocolos utilizados por Samba. (Helsin, 2013, p.04).

- **NetBIOS**

  *NetBIOS* es un protocolo antiguo para la prestación de servicios en la capa de sesión de modelo *OSI*. *NetBIOS* ofrece tres servicios: se*rvicio de nombres*, *servicio de sesión* y *servicio de datagramas*. (Helsin, 2013, p.88).

# CAPÍTULO III. ESTADO DEL ARTE METODOLÓGICO

## 1. Modelos de control de acceso

Según el tipo de política de autorización, los modelos de control de acceso pueden ser divididos en: modelos de control de acceso tradicional, modelo de control de acceso basado en roles y modelo de control de acceso basado en atributos.

### *1.1. Modelos tradicionales de control de acceso*

Existen dos tipos de modelos tradicionales de control de acceso, los cuales son: el modelo de control de acceso discrecional o *Discretionary Access Control* (*DAC*), y el modelo de control de acceso mandatario o *Mandatatory Access Control* (*MAC*).

Yang-Feng et al. (2013) describen que la idea principal del modelo *DAC*, es que el sujeto (se un usuario o un proceso) del sistema, de manera autónoma puede otorga su propio acceso hacia algún objeto (en su totalidad o parcialmente) a otros actores. Su implementación se realiza generalmente estableciendo una matriz de control de acceso al sistema. En esta matriz, las filas corresponden a los sujetos del sistema, las columnas corresponden a los objetos del sistema y las celdas representan a los derechos de acceso hacia los objetos por los sujetos. (p.09).

Por otro lado, Tounis et al. (2014) describen que en el modelo de control de acceso mandatario, una autoridad central está al mando de dar las decisiones de acceso a un sujeto que solicite el acceso hacia algún objeto o hacia alguna información de los objetos. Con el fin de garantizar el acceso a los objetos y a la información que fluye entre ellos, el modelo de control de acceso mandatario asigna una etiqueta de acceso a cada sujeto y objeto. Una etiqueta de acceso es un nivel de seguridad que se utiliza para asegurar el flujo de información entre los objetos y sujetos con una relación de dominación. Estas etiquetas de seguridad que se utilizan para clasificar los objetos en función a la sensibilidad de la información que tienen. Las autorizaciones de los sujetos son los niveles de seguridad que se utilizan para reflejar la confiabilidad o las reglas de los sujetos. (p.47).

## *1.2. Modelo de control de acceso basado en roles*

Yang-Feng et al. (2013) describen que el control de acceso basado en roles o *Role Based Access Control*, simplifica la gestión de autorización en diferentes ambientes. En los sistemas *MAC* o *DAC*, los permisos de acceso se conceden directamente al usuario. Mientras que el número de usuarios en el sistema es grande y cambiante, la complejidad en la gestión de autorización aumenta. El control de acceso basado en roles asigna los derechos de acceso a un rol. Los roles son relativamente estables en comparación a los usuarios. El rol de hecho es asociado con un conjunto de opciones de permisos en particular. Cuando los usuarios cambian, los roles solo necesitan ser retirados y reasignados. (p.09).

Del mismo modo, Tounis et al. (2014) describen que el modelo de control de acceso basado en role*s*, es considerado como una forma natural de controlar el acceso a los recursos en las organizaciones y empresas. La motivación detrás de modelo de control de acceso basado en roles parte de considerar que "la responsabilidad de un sujeto es mas importante que el sujeto en si". En el modelo, un sujeto puede tener más de un rol o ser miembro de varios grupos. Finalmente, el modelo de control de acceso basado en roles tiene muchas ventajas en comparación con los otros modelos, sin embargo, tiene sus propias dificultades cuando se despliega en el mundo real. En primer lugar, la selección de los roles correctos que representan a un sistema no es una tarea fácil, y la división de los sujetos en categorías basadas en los roles podría empeorar las cosas. Los roles en el modelo, clasifican a los sujetos en una serie de categorías; así, cada sujeto tiene que tener un rol con el fin de acceder al sistema. A pesar de eso, los roles pueden dar  a un sujeto más derechos que los que necesita necesariamente tener, con la posibilidad de tener otro rol que podría conducir a la violación de una política de acceso. (p.48).

### *1.3. Modelo de control de acceso basado en atributos*

Yang-Feng et al. (2013) describen que los elementos básicos de control de acceso basado en atributos o *Attribute Based Access Control*, incluye a los recursos solicitados que se quieren acceder, los métodos de acceso y las condiciones. El sistema utiliza a los atributos para describir estos elementos y los atributos asociados de cada elemento pueden ser definidos de acuerdo con el sistema. El concepto de control de acceso basado en atributos unifica la descripción de todos los elementos y ayuda al sistema a librarse de las restricciones basadas en la identidad. (p.09).

Del mismo modo, Tounis et al. (2014) describen que el modelo de control de acceso basado en atributos, se basa en un conjunto de atributos asociados a un solicitante o a un recurso a ser visitado, con el fin de tomar las decisiones de acceso. Hay muchas maneras de definir o utilizar los atributos en este modelo. Un atributo puede ser un trabajo, fecha de inicio de un usuario, una ubicación de un usuario, un rol de un usuario o de todos ellos. Los atributos pueden también estar o no relacionados entre sí. Después de definir los atributos que se utilizaran en el sistema, cada atributo es considerado como un valor discreto, y los valores de todos los atributos se comparan con un conjunto de valores para un punto de decisión de una política de conceder o denegar algún acceso En este tipo de modelo, un sujeto no tiene que ser conocido con anticipación por el sistema, sólo tiene que autenticarse en el sistema y luego proveer sus atributos. Por último, ellos describen que tener una política de seguridad que pueda funcionar con precisión con este tipo de modelo de control de acceso es vital, debido a que la política de seguridad es responsable de seleccionar a los atributos importantes que se utilizaran para tomar las decisiones de acceso. (p.48).

## 2. Sistemas de control de acceso

### *2.1. Windows Server 2008 R2 con Active Directory*

*Windows Server 2008 R2* es un sistema operativo empresarial de *Microsoft* para empresas y provee característica de virtualización, ahorro de energía, gestionabilidad y acceso desde dispositivos móviles. *Windows Server 2008 R2* esta disponible en diferentes ediciones tales como: Foundation, Standard, Enterprise, Datacenter, Web y HPC (High Performance Computing). (Heslin, 2013, p.08).

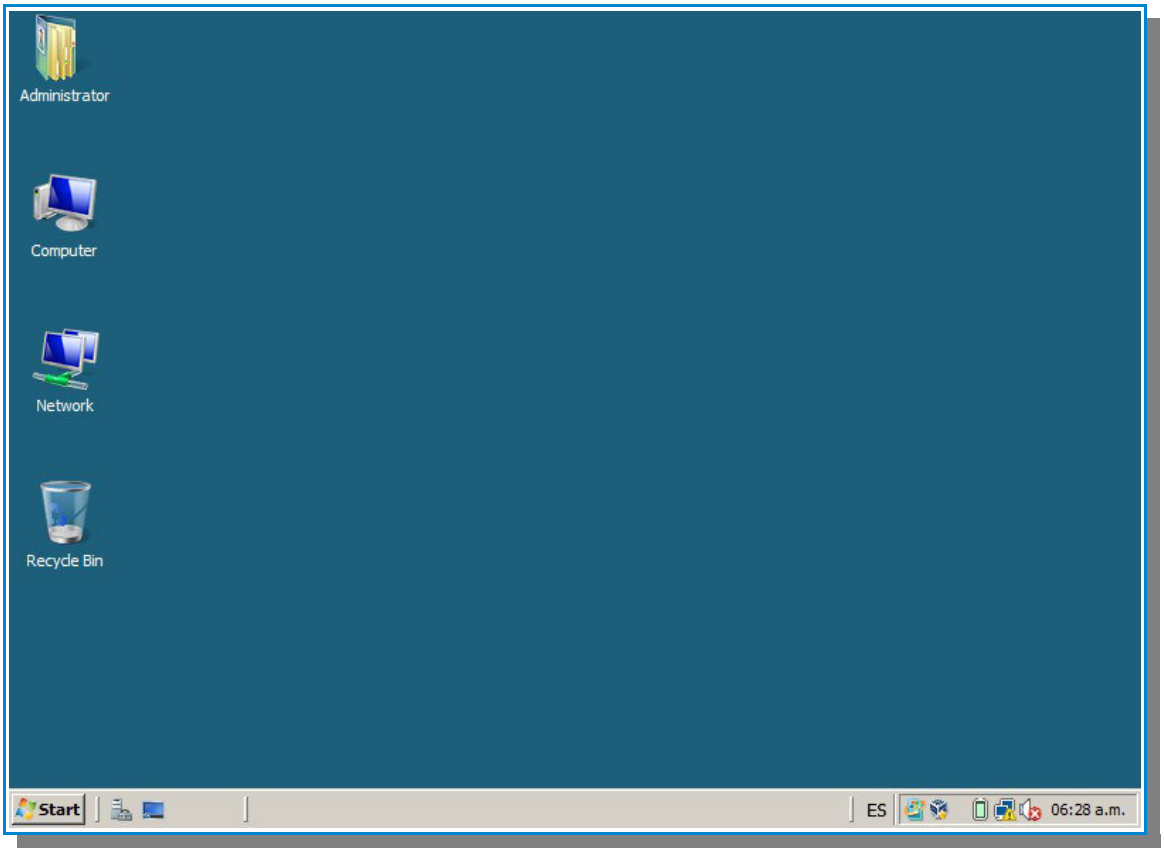


Figura 1: Windows Server 2008 R2

*Active Directory Domain Services* es una colección de servicios de directorio desarrollado por *Microsoft* que utiliza versiones personalizadas de los protocolos estándar en la industria de TI, incluyendo: *Kerberos*, *Domain Name* System, Lightweight *Directory Access Protocol*. A su vez, *Active Directory* permite a los administradores de sistemas *Windows* gestionar de forma segura los objetos del directorio desde una infraestructura de base de datos centralizada y escalable. Los objetos del directorio son almacenados en una jerarquía consistente de nodos, árboles y dominios. (Heslin, 2013, p.08).

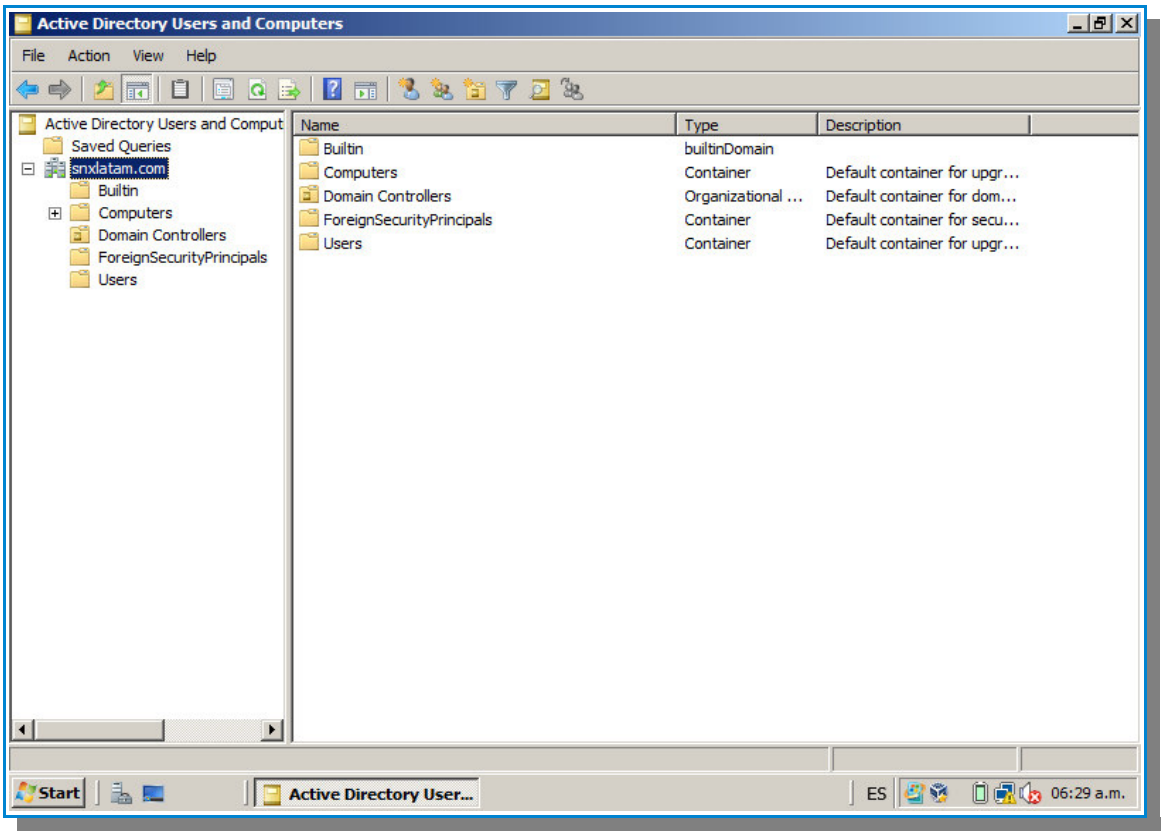


Figura 2: Active Directory Domain Services

## *2.2. Red Hat Enterprise Linux 7 con Identity Management*

*Red Hat Enterprise Linux* organiza los recursos de hardware que cumplen con los requisitos informáticos básicos de la infraestructura, tales como la CPU, la memoria, la red y el almacenamiento. *Red Hat Inc.* trabaja estrechamente con ingenieros de los principales proveedores de hardware para asegurarse de que el sistema operativo aproveche al máximo las innovaciones de hardware más recientes. Gracias a esta colaboración, cuando se presenta un nuevo diseño de chip, arquitectura de sistema o controlador que acelere el rendimiento u optimiza la energía, *Red Hat Enterprise Linux* puede cumplir con las especificaciones. ("Datasheet, Red Hat", 2014, p.01).

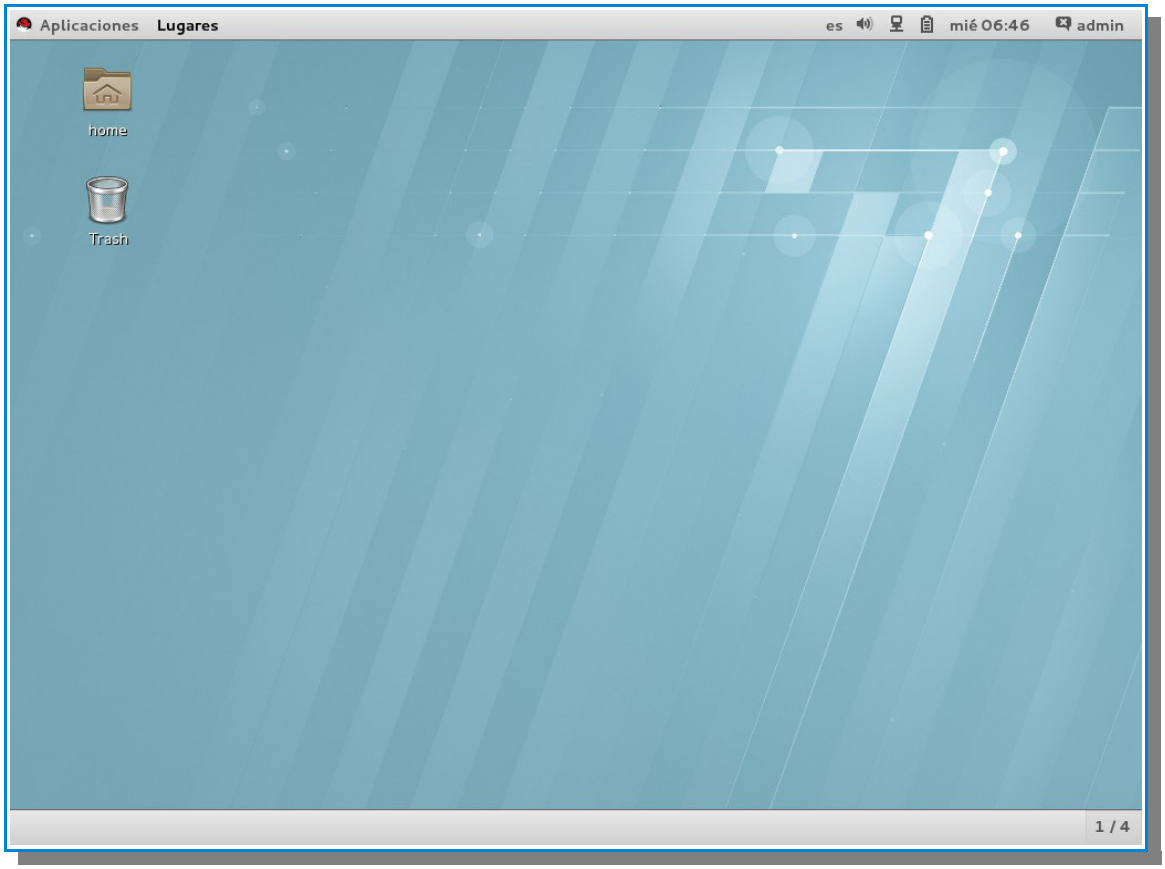


Figura 3: Red Hat Enterprise Linux 7

*Red Hat Identity Management* presenta un marco unificador para los servicios de red comunes definidos por estándares, incluidos *LDAP*, *Kerberos*, *DNS*, *NTP* y servicios de certificados. Esto permite que cualquier sistema *Red Hat Enterprise Linux* actúe como un controlador de dominio en un entorno *Linux*. Los controladores de dominio pueden ofrecer un inicio de sesión único de nivel empresarial, gestión de certificados, integración con *DNS* e interfaces de usuario (IU) de línea de comandos y web para la gestión de identidades, certificados y claves. ("Informe Tecnológico, Red", 2014, p.01).

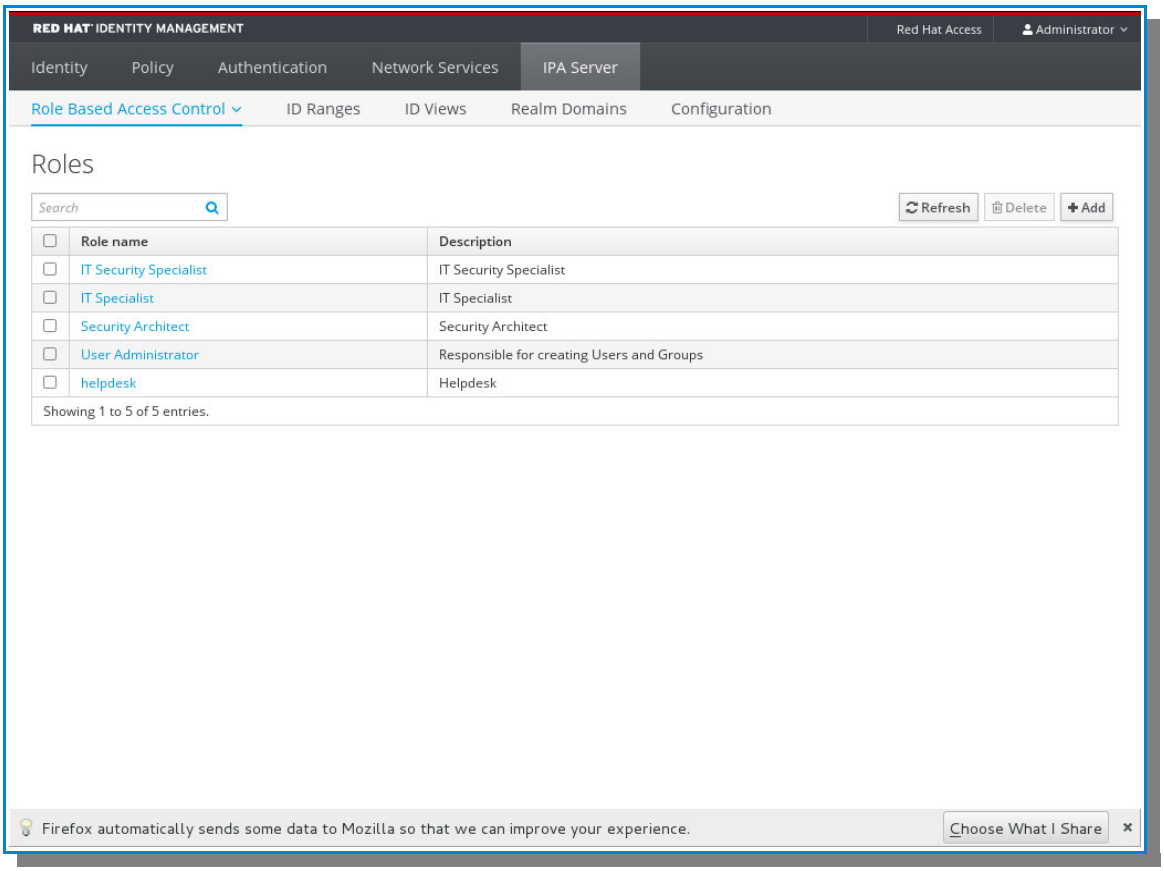


Figura 4: Red Hat Identity Management

## 3. Casos de estudio

### *3.1. Modelo extendido de control de acceso para un sistema de gestión del conocimiento*

Wang et al. (2014) en el artículo *Extended access control and recommendation methods for enterprise knowledge management system*, propusieron un modelo extendido de control de acceso basado en roles para un sistema empresarial de gestión del conocimiento. Al modelo de control de acceso basado en roles, los autores incluyen una estructura de grupos de usuarios, la cual a su vez era dividida en dos tipos de grupos, esto con el fin de que los usuarios puedan ser agregados a los dos tipos diferentes, y los privilegios puedan ser otorgados tanto a los grupos de usuarios como a los roles. Dentro del sistema de gestión del conocimiento, los autores determinaron que existe de dos tipos de restricciones para los usuarios: una referente a las funciones del sistema que pueden utilizar, y otra referente a la información que pueden acceder. Para manejar estas restricciones, introducen un esquema de tres capas en el modelo de control de acceso basado en roles (una capa para usuarios, una capa para roles y otra para grupos). La capa de roles se utilizara para gestionar las restricciones referentes al acceso a las funciones del sistemas, mientras que la capa de grupos servirá para gestionar las restricciones referentes al acceso a la información.

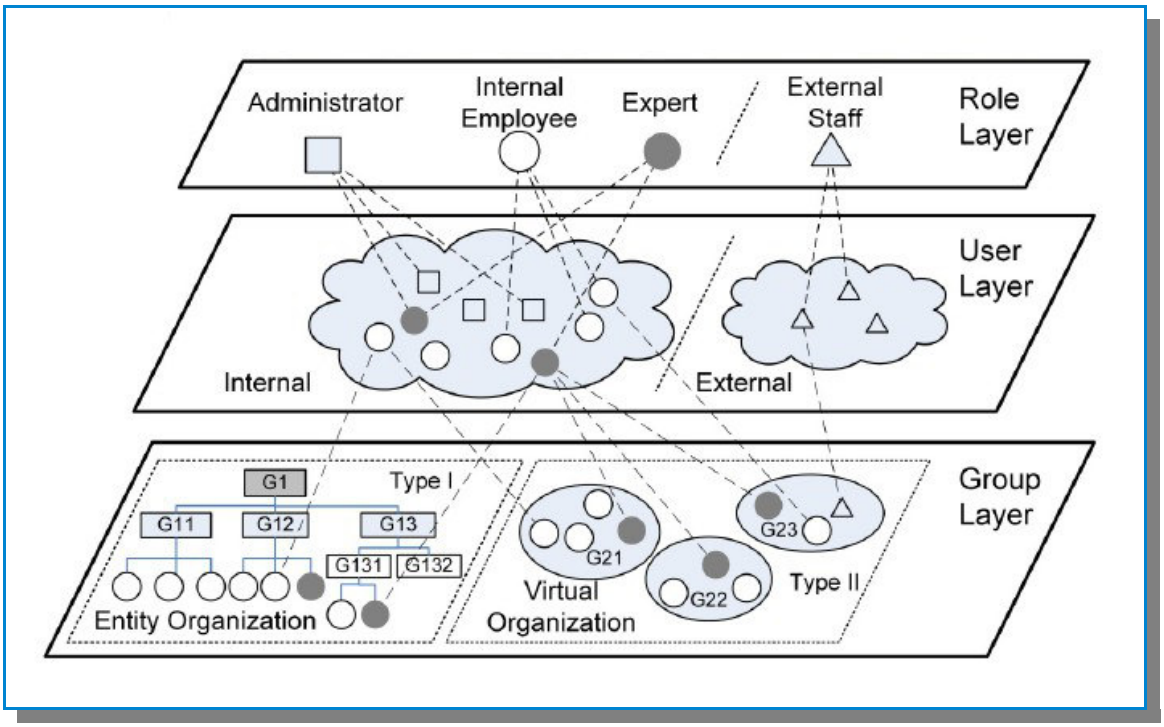


Figura 5: Esquema de tres capas para el sistema de gestión del conocimiento

### *3.2. Control de acceso para una plataforma de trabajo colaborativo*

Yan-Feng et al. (2013) en el artículo *Access control for rural medical and health collaborative working platform*, propusieron un modelo de control de acceso basado en diferentes tipos de usuarios o roles para una plataforma de trabajo colaborativo. El modelo de control de acceso para la plataforma de trabajo colaborativo estuvo definido por tres elementos principalmente: un conjunto de usuarios (compuesto por los usuarios del sistema o cualquier otra entidad que actué como un usuario), un conjunto de objetos (compuesto por los recursos del sistema) y un conjunto de operaciones (compuesto por entidades que definen que es lo que se debe hacer). Dentro de la plataforma de trabajo colaborativo, cada modulo que lo compone trabaja en una maquina virtual aparte, pero interactuá con los demás. Los autores determinaron que el personal que necesita tener acceso a la información privada de los usuarios, también necesita tener diferentes permisos acceso para cada módulo. Para manejar este restricción, determinan que el modelo de control de acceso propuesto debería de estar embebido en cada uno de los cuatro módulos que componen la plataforma trabajo colaborativo, esto con el fin de hacer que la plataforma trabaje de manera más efectiva y segura, ya que cada modulo maneja un conjunto de usuarios con diferentes permisos acorde a los variedad roles de usuarios que albergan.

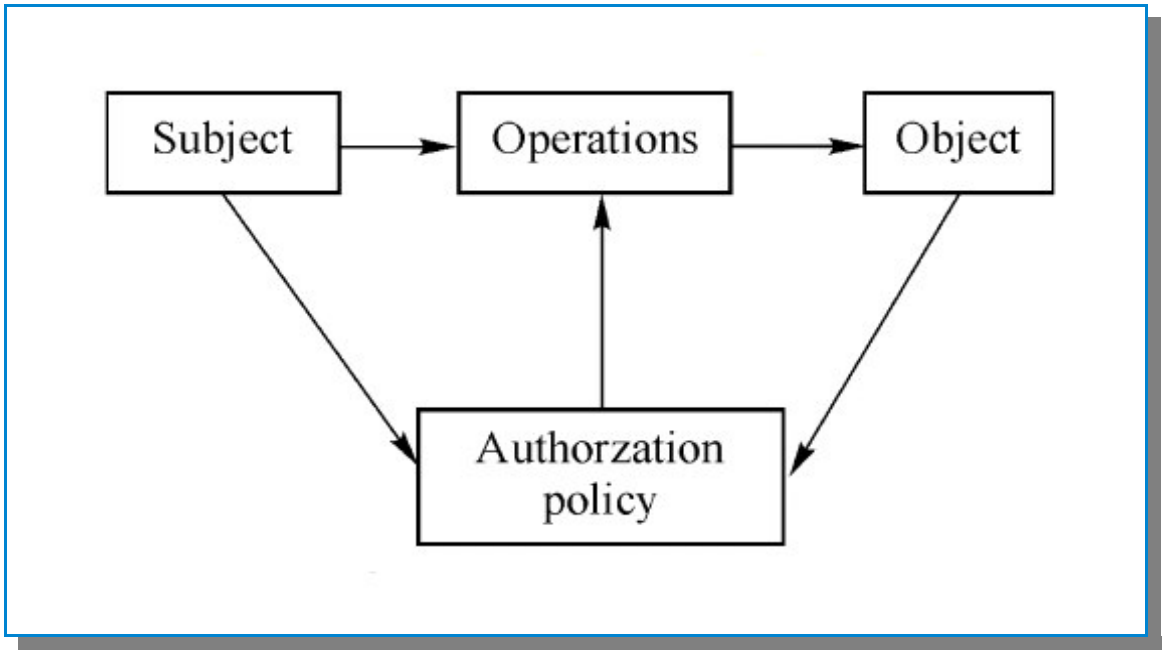


Figura 6: Modelo de control de acceso para la plataforma de trabajo colaborativo

### *3.3. Una mejora al modelo de control de acceso basado en roles*

Hung et al. (2012) en el artículo *An enhancement of the Role-based access control model to facilitate information access management in context of team collaboration and workflow*, propusieron una mejora al modelo de control de acceso basado en roles para facilitar la gestión de acceso a la información dentro de un contexto de colaboración y trabajo en equipo. El modelo mejorado de control de acceso, contó con la formulación de restricciones universales (que son colecciones de restricciones que regulan los aspectos específicos del control de acceso), definición de clara de entidades, extensión de permisos de acceso para apuntar a objetivos específicos y el desarrollo de ontologias del dominio (el cual define las instancias especificas que se derivan del modelo general, para implementarlas en un dominio o escenario en particular, la relación que puede haber entre dominios y las restricciones sobre los componentes y las relaciones). Los autores indican que en este trabajo se aplico de forma exitos del modelo RBAC mejorado en el proyecto de "Iniciativa de educación clínica HIV" (CEI) del estado de New York para atender las necesidades específicas de gestión de acceso a la información en un contexto de colaboración y trabajo en equipo.

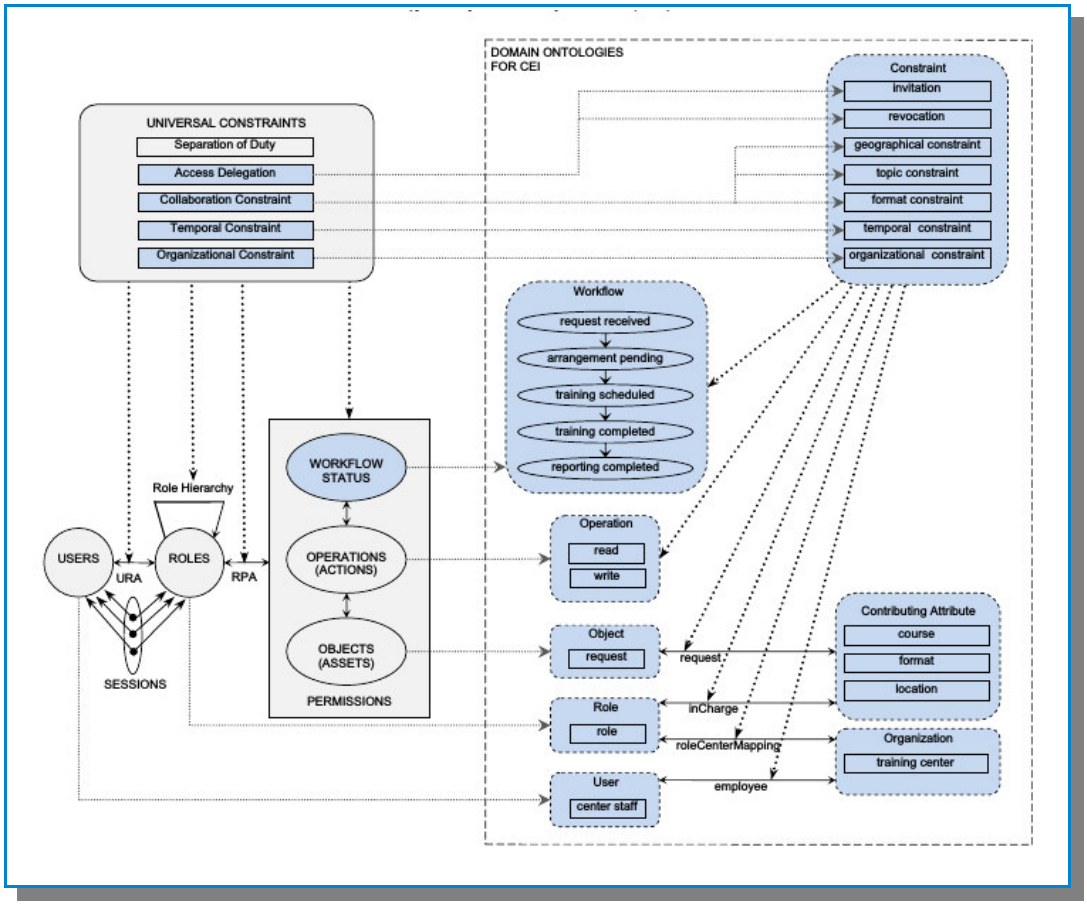

Figura 7: Modelo de control de acceso mejorado basado en roles para la plataforma

# CAPÍTULO IV. DESARROLLADO DE LA SOLUCIÓN O DEL ESTUDIO

## 1. Resolución del problema

### *1.1. Evaluación y selección del modelo*

#### *1.1.1. Modelo teóricos propuestos*

En base al estudio realizado en el *CAPÍTULO III. ESTADO DEL ARTE METODOLÓGICO*, se pudo identificar la presencia de dos modelos de control de acceso que son básicamente los más representativos en este campo y que podrían aplicarse para la resolución de nuestro problema. Estos modelos de control de acceso son los siguientes:

- Modelo de control de acceso basado en roles.
- Modelo de control de acceso basado en atributos.

A continuación pasaremos a desarrollar los criterios de selección para poder definir los puntos sobre los cuales seleccionaremos al modelo más adecuado para el desarrollo del presente proyecto.

#### *1.1.2. Criterios de selección*

Para la selección del modelo de control de acceso, se tomara en cuenta los siguientes criterios: *capacidad*, *compatibilidad* y *complejidad*; los cuales definiremos a continuación:

- ***Capacidad.-*** Relacionado a las propiedades que tienen el modelo en materia de seguridad de la información.
- ***Compatibilidad.-*** Relacionado a la compatibilidad con el entorno en donde se desee implementar gestión de acceso.
- ***Complejidad.-*** Relacionado a la complejidad en el diseño del modelo de control de acceso final.

### *1.1.3. Análisis comparativo*

En esta sección se realizara un análisis comparativo entre los sistemas de control de acceso, tomando en cuenta los criterios de selección previamente establecidos y la información revisada (Smari et al., 2014; Gouglidis et al., 2012) en la bibliografía.

| | **Modelo de control de acceso basado en roles (RBAC)** | **Modelo de control de acceso basado en atributos (ABAC)** |
|---|---|---|
| **Capacidad** | Incluye solo las propiedades que son más relevantes para la seguridad. | No ha sido estandarizado y estudiado a profundidad todavía. |
| **Compatibilidad** | Es compatible con varios entornos en los que se desee implementar control de acceso, ya que sigue un enfoque jerárquico. | Es principalmente compatible en entornos de sistemas distribuidos. |
| **Complejidad** | Es más complejo de elaborarlo, pero cuando se genera trabaja muy bien en cualquier tipo de organización. | Es menos complejo elaborar el modelo pero solo funciona en organizaciones que no son grandes. |

En relación a a información expuesta en el análisis comparativo realizado, hemos optado en utilizar al modelo de control de acceso basado en roles como base para el diseño de nuestra solución de sistema de control de acceso.

### *1.2. Aplicación del modelo*

Goncalves et al. (2007) define que debido a que el lenguaje *UML* tiene la posibilidad de presentar un sistema utilizando diferentes tipos de modelos, proponen utilizar las propiedades de este lenguaje para reproducir el modelo de control de acceso basado en roles (*RBAC*) relacionado a nuestro caso de estudio. Para lograr esto, primero se debe relacionar a los conceptos del lenguaje *UML* con los del modelo *RBAC*. Luego, dos tipos de diagramas *UML* son utilizados para elaborar el modelo RBAC final: el diagrama de casos de uso y el diagrama de secuencia (p.1311).

#### *1.2.1. Relación entre conceptos*

- **Roles - Actores**

  En el lenguaje *UML*, un actor define como un función o un conjunto de funciones son desempeñados por una persona o por un grupo de personas que interactúan con el sistema. Así cada usuario específico o grupos de usuarios puede ser tratado como un actor. Sin embargo, ya que los usuarios pueden desempeñar diferentes funciones, esto deriva en que un actor también pueda ser visto como un actor. (Goncalves et al., 2007, p.1311).

- **Funciones – Casos de uso**

  Las funciones son representadas en el *UML* a través de los casos de uso. Cada actor se relaciona con uno o más casos de uso que representan las funciones esenciales de un sistema. Es por eso que un caso de uso puede ser visto como una función dentro del modelo *RBAC* diseñado. (Goncalves et al., 2007, p.1312).

- **Métodos y objetos**

  Los métodos en el modelo *RBAC* están representados en el lenguaje *UML* por los métodos que se ejecutan en los diferentes tipos de diagramas (diagrama de secuencia, diagrama de colaboración, etc.), mientras que para los objetos del modelo *RBAC* se utiliza el mismo concepto de objeto de *UML*. (Goncalves et al., 2007, p.1312).

- **Permisos – Diagramas de secuencia**

  Un caso de uso contiene una secuencia de acciones ejecutadas por un actor de un sistema. Es por eso que los diagramas de secuencia han sido elegido para describir con mayor detalle, el interior de los casos de uso. Un diagrama de secuencia representa una interacción de objetos por medio de una secuencia de mensajes enviados entre estos objetos. Cuando se produce la recepción de un mensaje, se activa la ejecución de un método respectivamente. Para cada actor, el modelo de control de acceso permite especificar una lista de métodos que el actor puede ejecutar. Por lo tanto, para cada caso de uso es necesario especificar los permisos relacionados a la ejecución del método. En la mayoría de los casos sólo un actor; principalmente el que inicia la interacción; tiene la mayoría de los permisos. El segundo actor o los otros actores que participan en la misma interacción tienen sólo una parte de los permisos de la misma. (Goncalves et al., 2007, p.1312).

### *1.2.2. Creación de roles*

Para conocer el nombre de los roles iniciales, se hará uso de un diagrama de caso de uso del negocio, el cual nos definirá la lista de actores participantes en el servicio de "Gestión de proyectos y consultoría".

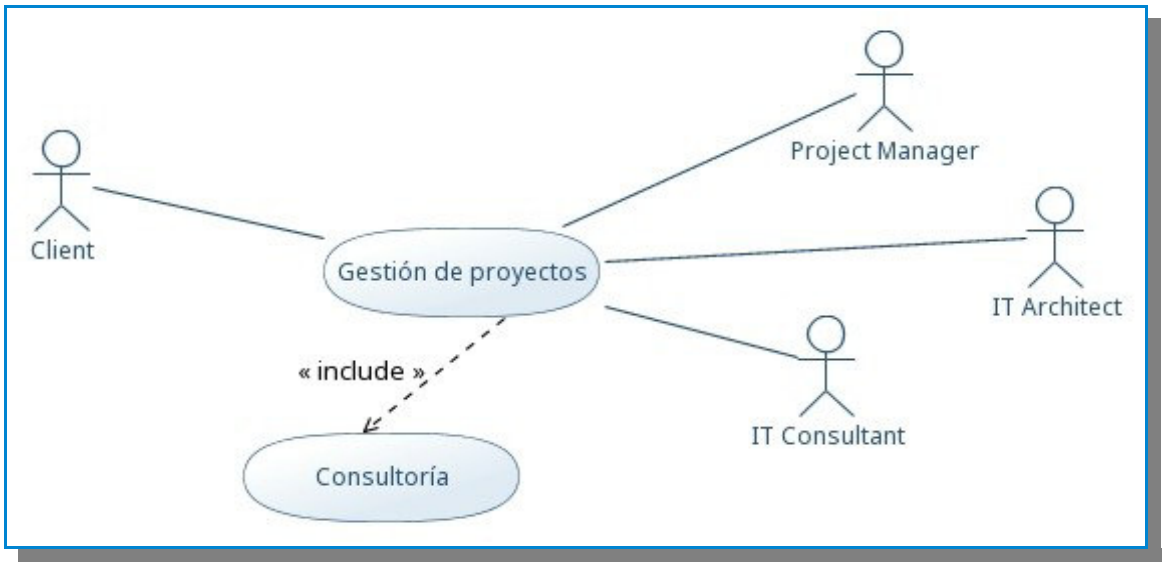


Figura 8: Diagrama de caso de uso "Servicio de gestión de proyectos y consultoría"

A continuación, presentamos la lista de roles obtenida:

- **Lista de roles:** “Project Manager”, “IT Architect”, “IT Consultant”.

Así también, podemos observar que el servicio de “Gestión de proyectos y consultoría” se puede dividir en dos sub servicios que son los siguientes:

- **Lista de funciones:** “Gestión de proyectos” y “Consultoría”.

Para concluir proceso de producción de roles, se necesitara ejecutar dos etapas adicionales, que permitirán definir las funciones y los permisos que tendrá cada rol dentro de los sub servicios identificados:

- La asignación del conjunto de casos de uso (funciones) a un actor (rol).
- La asignación del conjunto de privilegios (permisos) en un caso de uso (función) con el fin de terminar con su definición.

### *1.2.3. Definición de funciones asignadas a los roles*

Los diagramas de casos de uso permite la visualización del conjunto de funciones de un sistema mediante el examen de las necesidades de cada actor. Por lo tanto, el conjunto de relaciones establecidos dentro del diagrama de caso de uso, especificaran al conjunto de funciones que deben ser asignados a cada rol. (Goncalves et al., 2007, p.1314). A continuación presentaremos a los diagramas de caso de uso relacionados al servicio de "Gestión de proyectos y consultoría".

- **Caso de uso: Gestión de proyectos**

  El diagrama de caso de uso "Gestión de proyectos", representa a la metodología utilizada por la empresa para el desarrollo del proceso de gestión de proyecto, el cual forma parte del servicio de "Gestión de proyectos y consultoría".

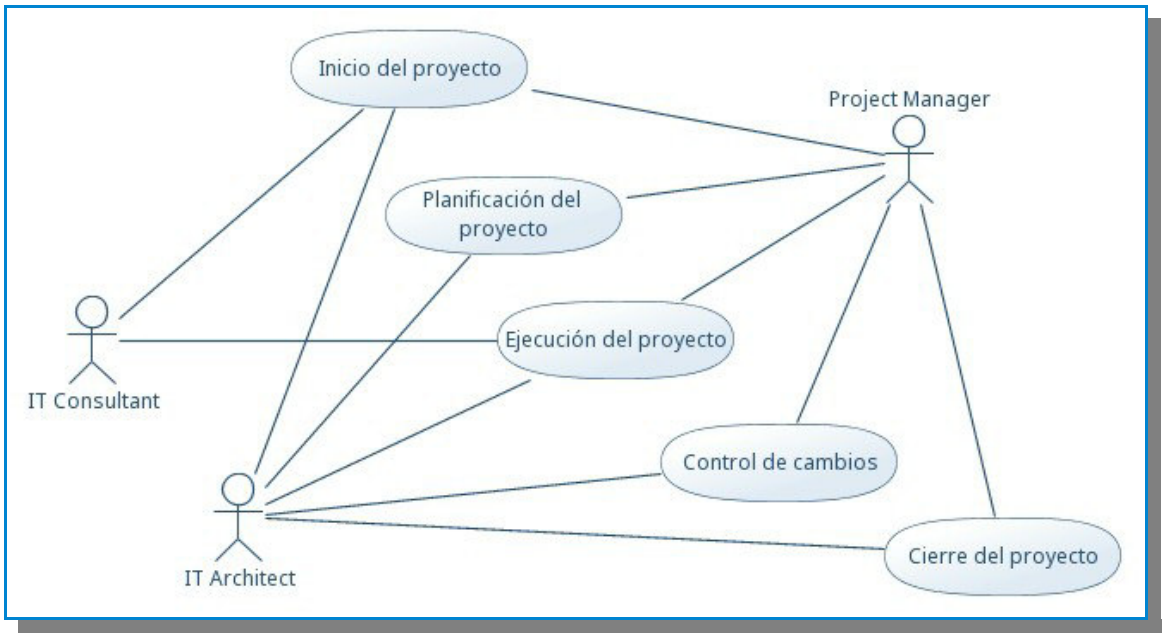


Figura 9: Diagrama de caso de uso "Gestión de proyectos"

Del presente diagrama podemos obtener a los actores y casos de uso, que representaran a los roles y funciones que formaran parte del modelo de control de acceso propuesto. Los conjuntos de roles y funciones obtenidos son los siguientes:

- **Roles:** “Project Manager”, “IT Architect”, “IT Consultant”.
- **Funciones:** “Inicio del proyecto”, “Planificación del proyecto”, “Ejecución del proyecto”, “Control de cambios”, “Cierre del proyecto”.

- **Caso de uso: Consultoría**

  Del mismo modo, el diagrama de caso de uso “Consultoría”, representa a la metodología utilizada por la empresa para el desarrollo del proceso de consultoría, el cual forma parte del servicio de “Gestión de proyectos y consultoría”.

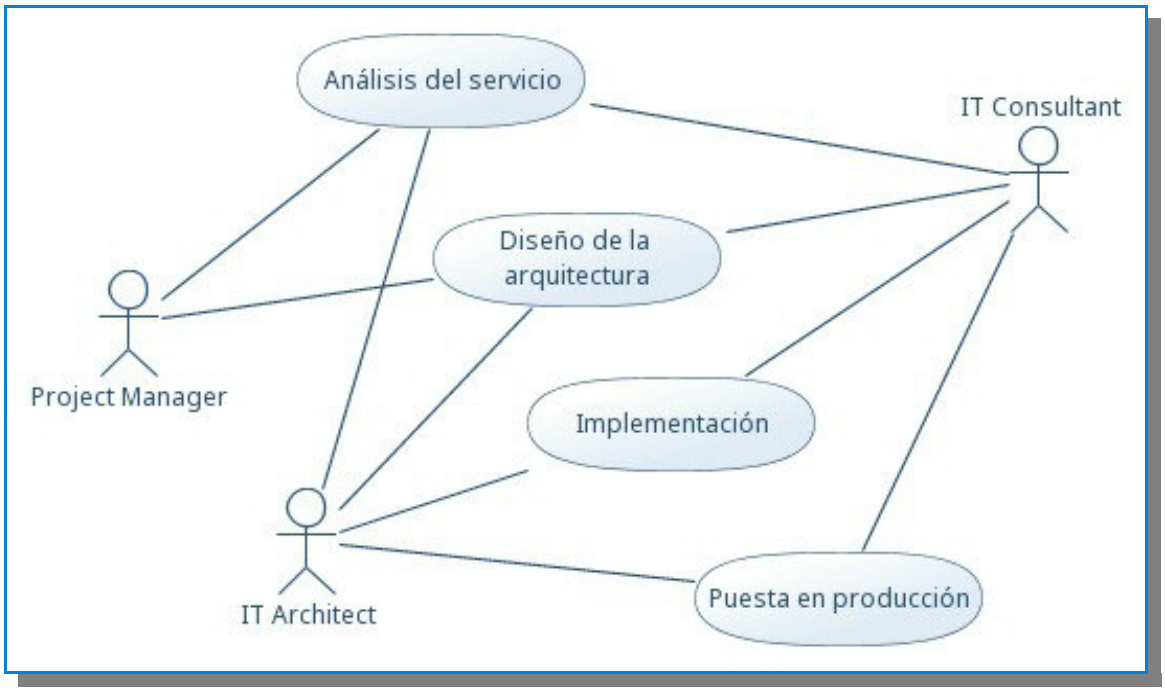


Figura 10: Diagrama de caso de uso "Consultoría"

Del presente diagrama podemos obtener a los actores y casos de uso, que representaran a los roles y funciones que formaran parte del modelo de control de acceso propuesto. Los conjuntos de roles y funciones obtenidos son los siguientes:

- **Roles:** “Project Manager”, “IT Architect”, “IT Consultant”.
- **Funciones:** “Análisis del servicio”, “Diseño de la arquitectura”, “Implementación”, “Puesta en producción”.

### *1.2.4. Definición de permisos asignados en las funciones*

Las interacciones entre los objetos dentro de un caso e uso, están representadas por una secuencia de acciones que permiten la definición de un conjunto de privilegios. Por lo tanto, con el fin de identificar los permisos asignados a una función, es necesario empezar desde el análisis de los diagramas de secuencia (Goncalves et al., 2007, p.1314). A continuación presentaremos a los diagramas de secuencia relacionados al servicio de "Gestión de proyectos y consultoría".

- ***Inicio del proyecto***

  Este diagrama de secuencia representa el comportamiento de los actores hacia los objetos, dentro del caso de uso "Inicio del proyecto". A partir de él, se puede obtener el conjunto de permisos asociados a los roles presentes en el modelo de control de acceso.

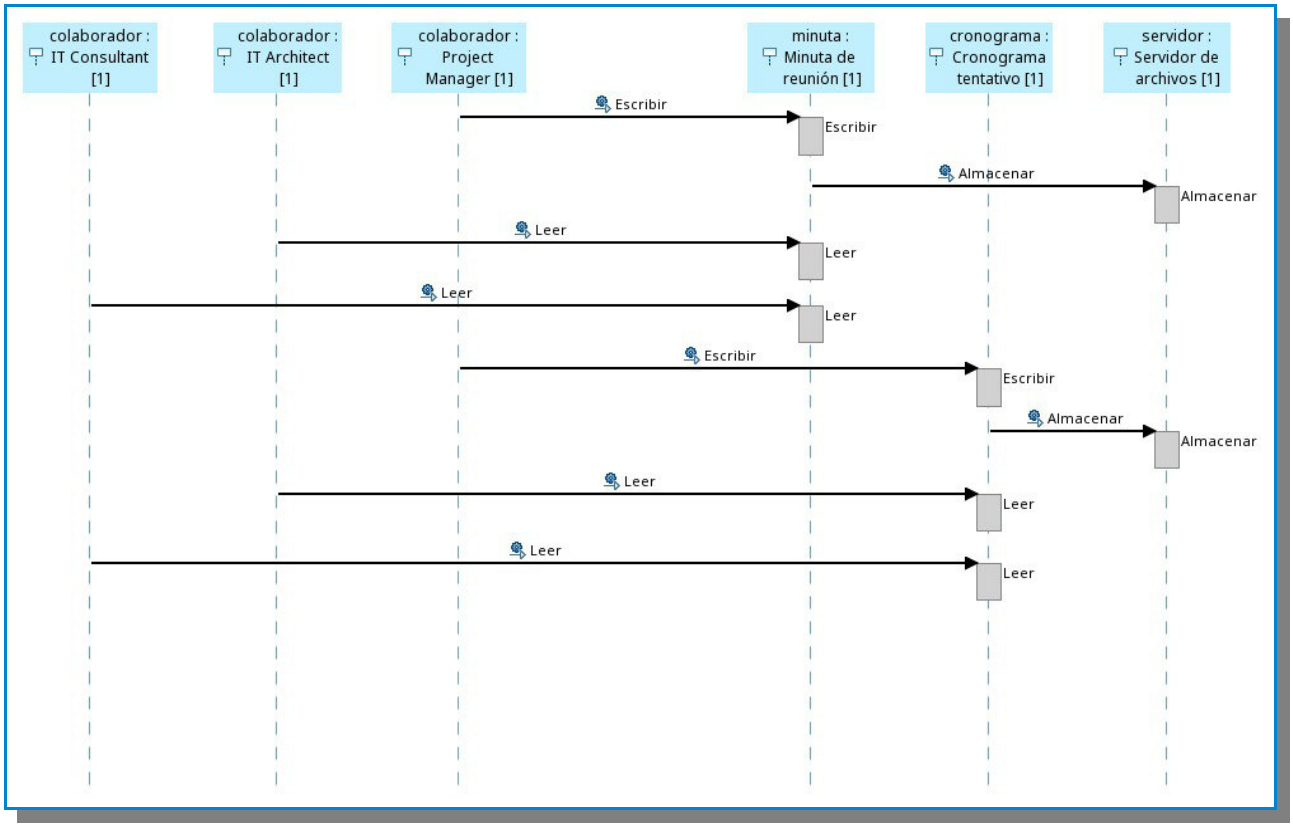


Figura 11: Diagrama de secuencia "Inicio del proyecto"

Los conjuntos de objetos, métodos y permisos obtenidos son los siguientes:

- **Objetos:** “Minuta de reunión”, “Cronograma tentativo”, “Servidor de archivos”.
- **Métodos:** “Escribir”, “Almacenar”, “Leer”.
- **Permisos:** (“Escribir”, “Minuta de reunión”), (“Leer”, “Minuta de reunión”), (“Escribir”, “Cronograma tentativo”), (“Leer”, “Cronograma tentativo”), (“Almacenar”, “Servidor de archivos”).

- ***Planificación del proyecto***

Este diagrama de secuencia representa el comportamiento de los actores hacia los objetos, dentro del caso de uso “Planificación del proyecto”. A partir de él, se puede obtener el conjunto de permisos asociados a los roles presentes en el modelo de control de acceso.

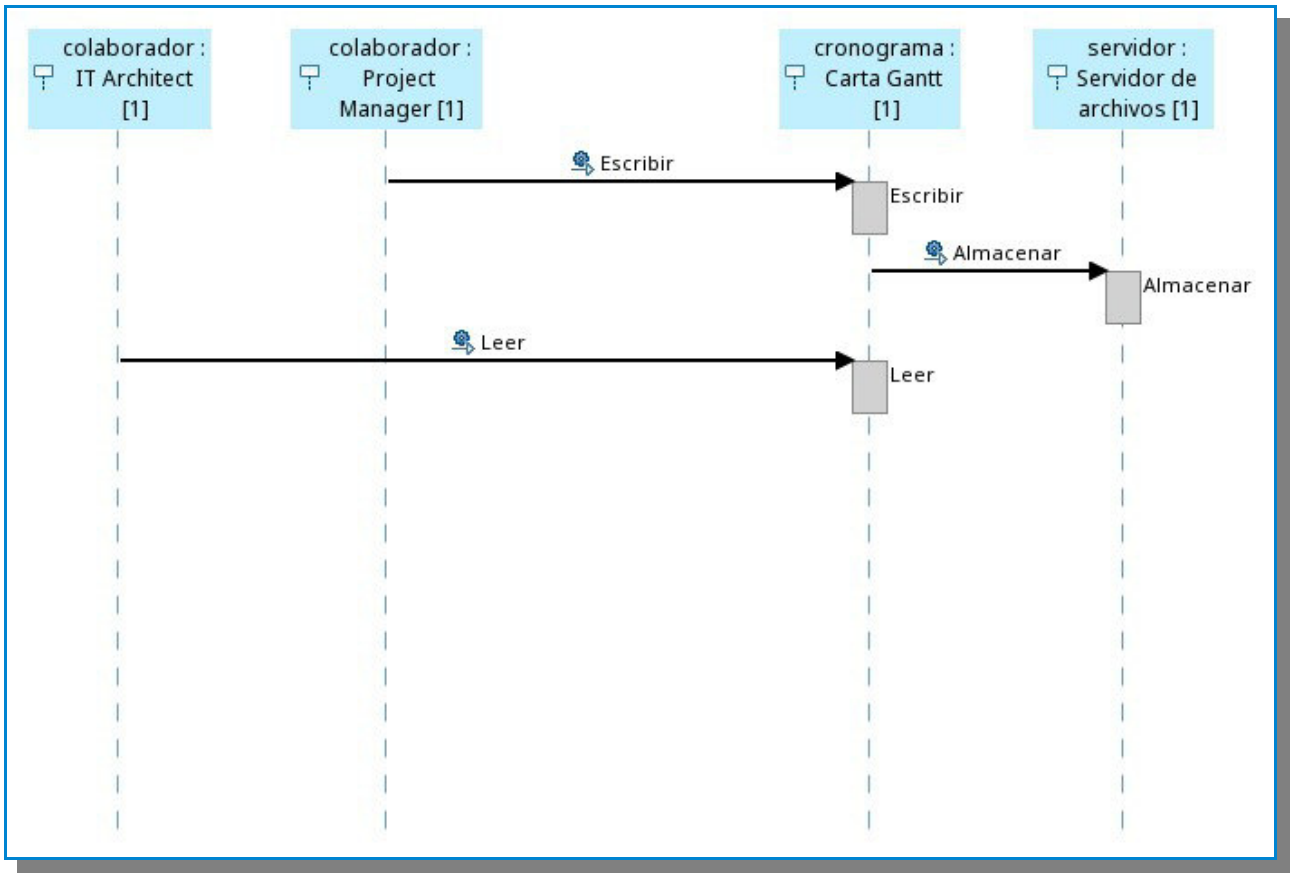


Figura 12: Diagrama de secuencia "Planificación del proyecto"

Los conjuntos de objetos, métodos y permisos obtenidos son los siguientes:

- **Objetos:** “Carta Gantt”, “Servidor de archivos”.
- **Métodos:** “Escribir”, “Almacenar”, “Leer”.
- **Permisos:** (“Escribir”, “Carta Gantt”), (“Leer”, “Carta Gantt”), (“Almacenar”, “Servidor de archivos”).

- ***Ejecución del proyecto***

  Este diagrama de secuencia representa el comportamiento de los actores hacia los objetos, dentro del caso de uso “Ejecución del proyecto”. A partir de él, se puede obtener el conjunto de permisos asociados a los roles presentes en el modelo de control de acceso.

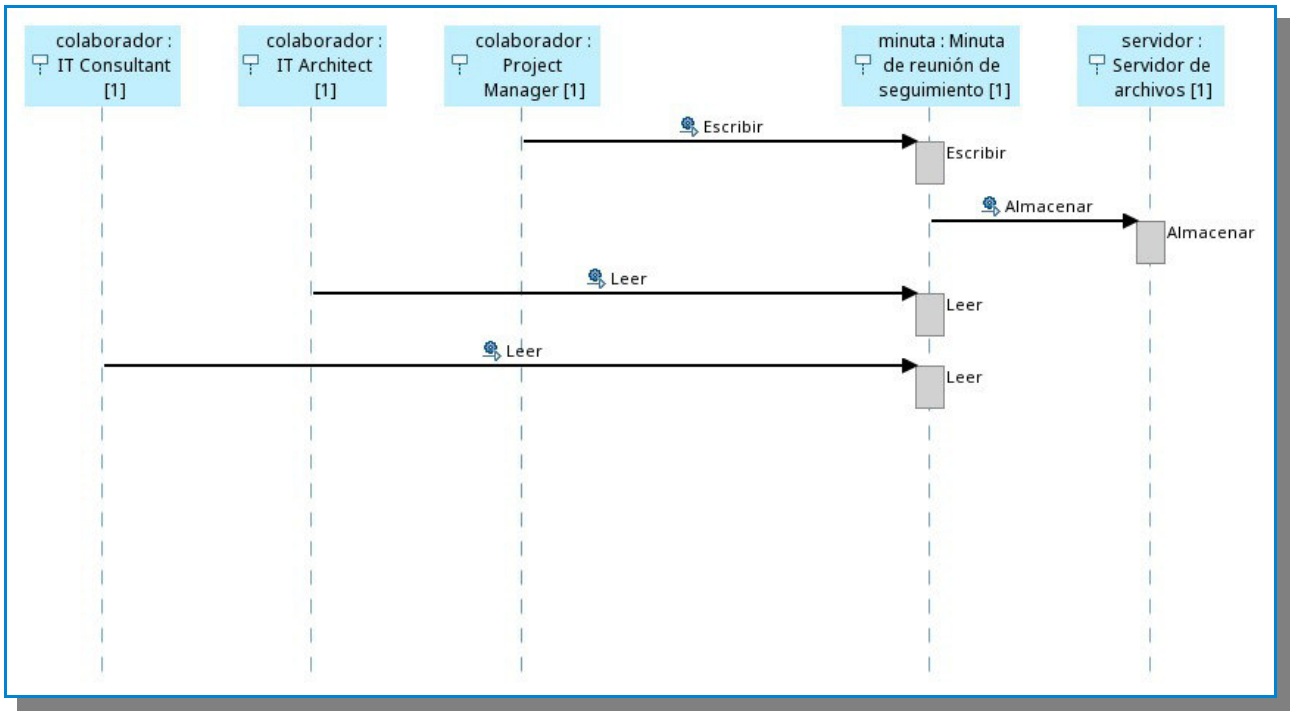


Figura 13: Diagrama de secuencia "Ejecución del proyecto"

Los conjuntos de objetos, métodos y permisos obtenidos son los siguientes:

- **Objetos:** “Minuta de reunión de seguimiento”, “Servidor de archivos”.
- **Métodos:** “Escribir”, “Almacenar”, “Leer”.
- **Permisos:** (“Escribir”, “Minuta de reunión de seguimiento”), (“Leer”, “Minuta de reunión de seguimiento”), (“Leer”, “Minuta de reunión de seguimiento”), (“Almacenar”, “Servidor de archivos”).

- ***Control de cambios***

  Este diagrama de secuencia representa el comportamiento de los actores hacia los objetos, dentro del caso de uso “Control de cambios”. A partir de él, se puede obtener el conjunto de permisos asociados a los roles presentes en el modelo de control de acceso.

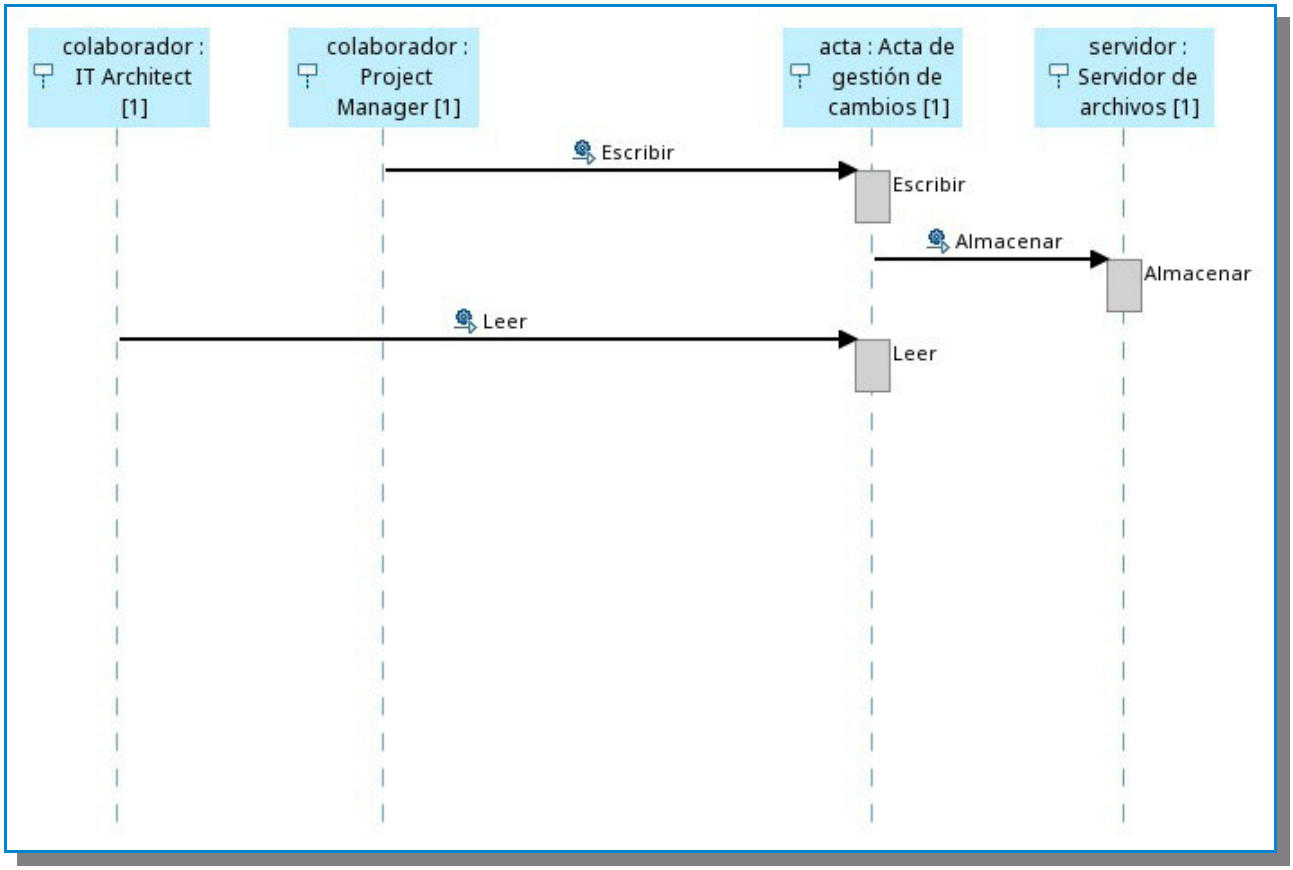


Figura 14: Diagrama de secuencia "Control de cambios"

Los conjuntos de objetos, métodos y permisos obtenidos son los siguientes:

- **Objetos:** “Acta de gestión de cambios”, “Servidor de archivos”.
- **Métodos:** “Escribir”, “Almacenar”, “Leer”.
- **Permisos:** (“Escribir”, “Acta de gestión de cambios”), (“Leer”, “Acta de gestión de cambios”), (“Almacenar”, “Servidor de archivos”).

- ***Cierre del proyecto***

  Este diagrama de secuencia representa el comportamiento de los actores hacia los objetos, dentro del caso de uso “Cierre del proyecto”. A partir de él, se puede obtener el conjunto de permisos asociados a los roles presentes en el modelo de control de acceso.

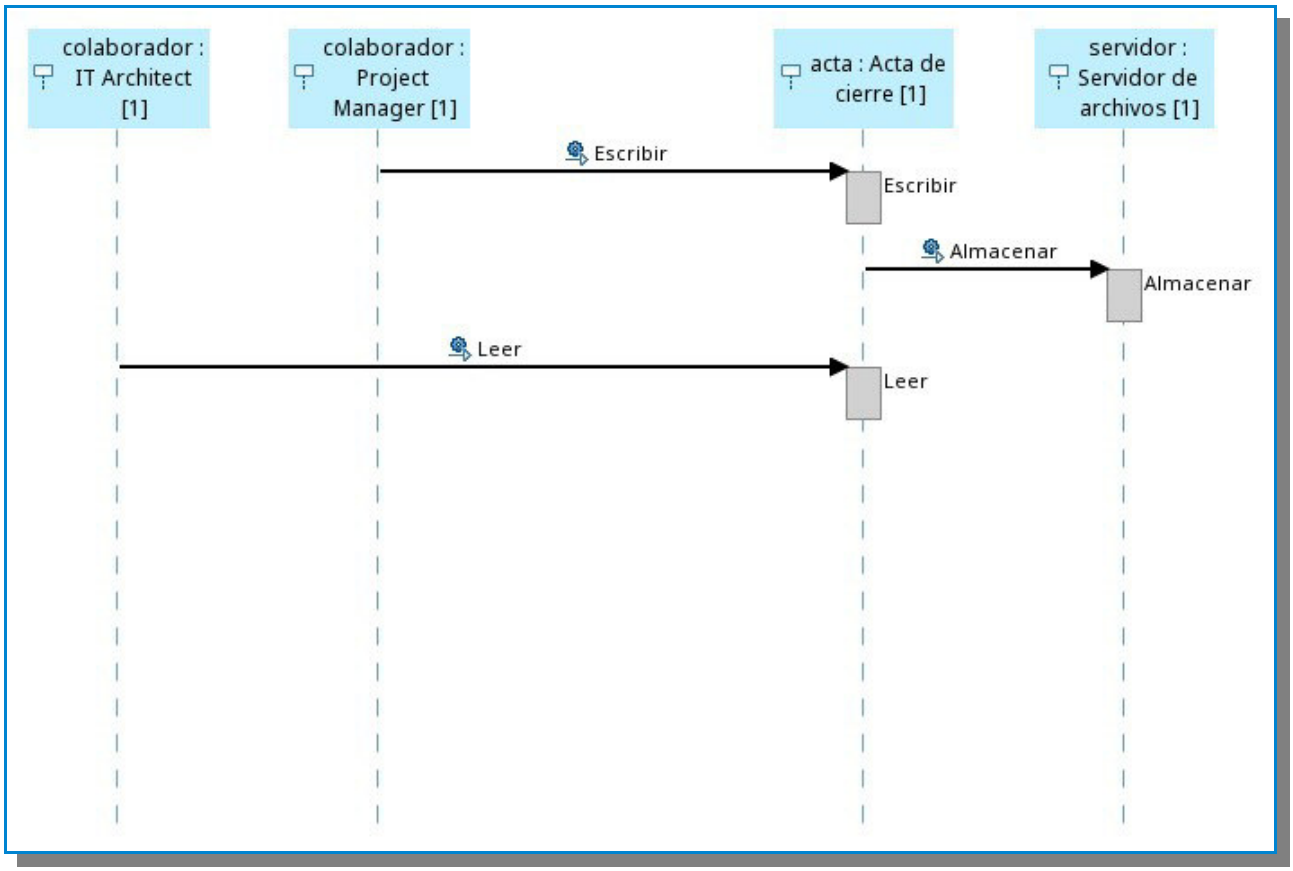


Figura 15: Diagrama de secuencia "Cierre del proyecto"

Los conjuntos de objetos, métodos y permisos obtenidos son los siguientes:

- **Objetos:** “Acta de cierre”, “Servidor de archivos”.
- **Métodos:** “Escribir”, “Almacenar”, “Leer”.
- **Permisos:** (“Escribir”, “Acta de cierre”), (“Leer”, “Acta de cierre”), (“Almacenar”, “Servidor de archivos”).

- ***Análisis del servicio***

  Este diagrama de secuencia representa el comportamiento de los actores hacia los objetos, dentro del caso de uso “Análisis del servicio”. A partir de él, se puede obtener el conjunto de permisos asociados a los roles presentes en el modelo de control de acceso.

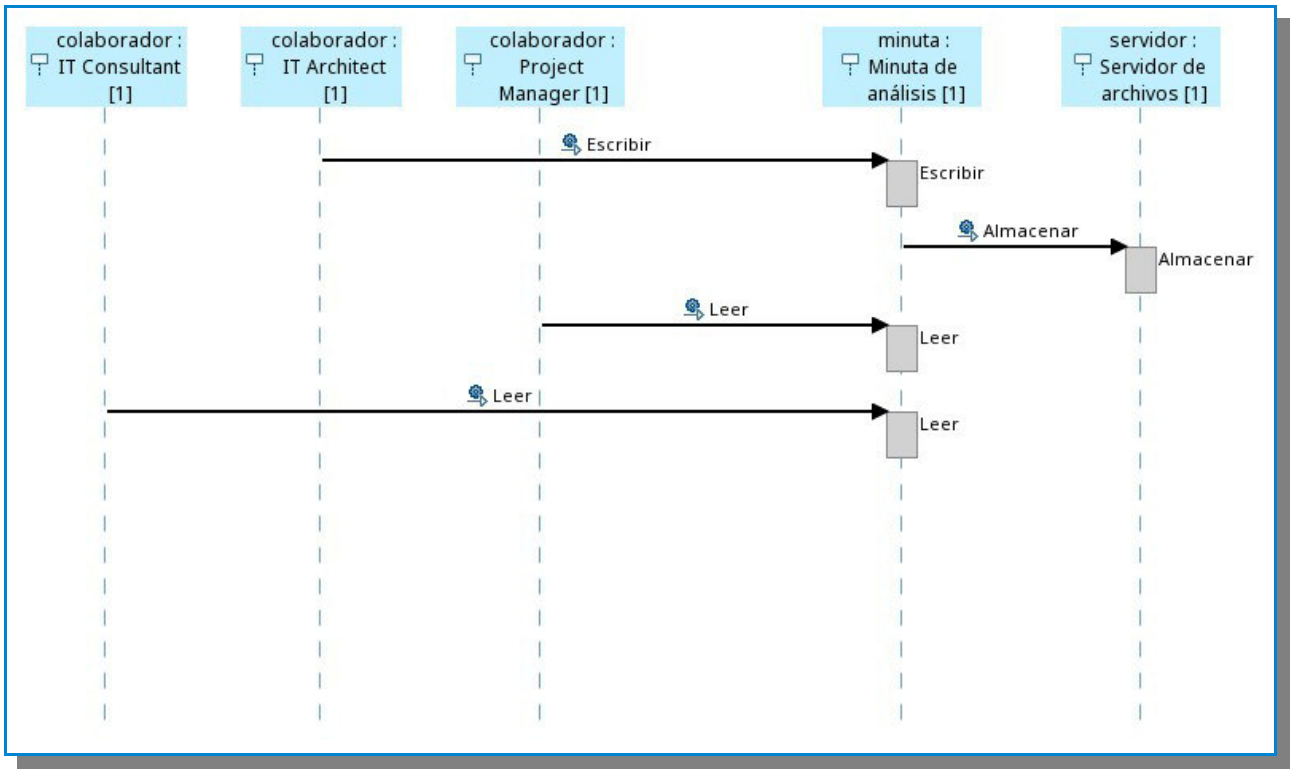


Figura 16: Diagrama de secuencia "Análisis del servicio"

Los conjuntos de objetos, métodos y permisos obtenidos son los siguientes:

- **Objetos:** “Minuta de análisis”, “Servidor de archivos”.
- **Métodos:** “Escribir”, “Almacenar”, “Leer”.
- **Permisos:** (“Escribir”, “Minuta de análisis”), (“Leer”, “Minuta de análisis”), (“Almacenar”, “Servidor de archivos”).

- ***Diseño de la arquitectura***

  Este diagrama de secuencia representa el comportamiento de los actores hacia los objetos, dentro del caso de uso “Diseño de la arquitectura”. A partir de él, se puede obtener el conjunto de permisos asociados a los roles presentes en el modelo de control de acceso.

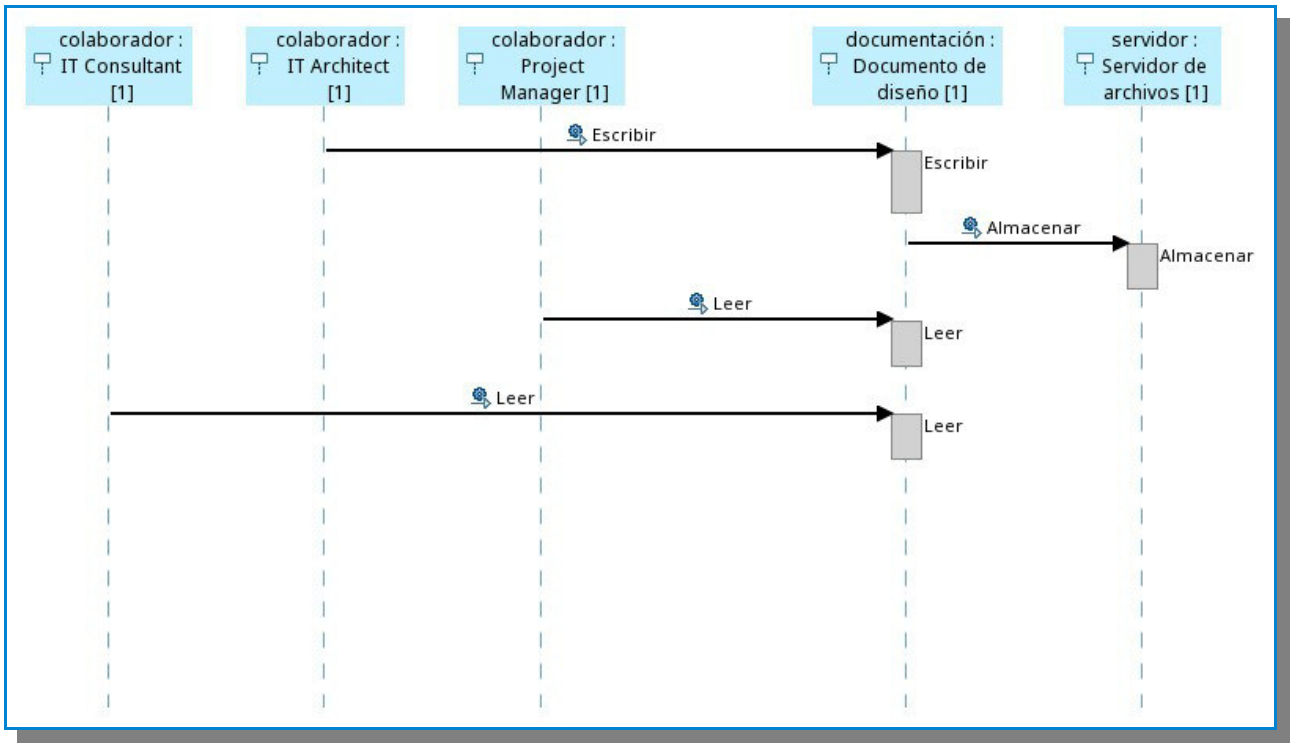


Figura 17: Diagrama de secuencia "Diseño de la arquitectura"

Los conjuntos de objetos, métodos y permisos obtenidos son los siguientes:

- **Objetos:** “Documento de diseño”, “Servidor de archivos”.

- **Métodos:** “Escribir”, “Almacenar”, “Leer”.
- **Permisos:** (“Escribir”, “Documento de diseño”), (“Leer”, “Documento de diseño”), (“Almacenar”, “Servidor de archivos”).

- ***Implementación***

  Este diagrama de secuencia representa el comportamiento de los actores hacia los objetos, dentro del caso de uso “Implementación”. A partir de él, se puede obtener el conjunto de permisos asociados a los roles presentes en el modelo de control de acceso.

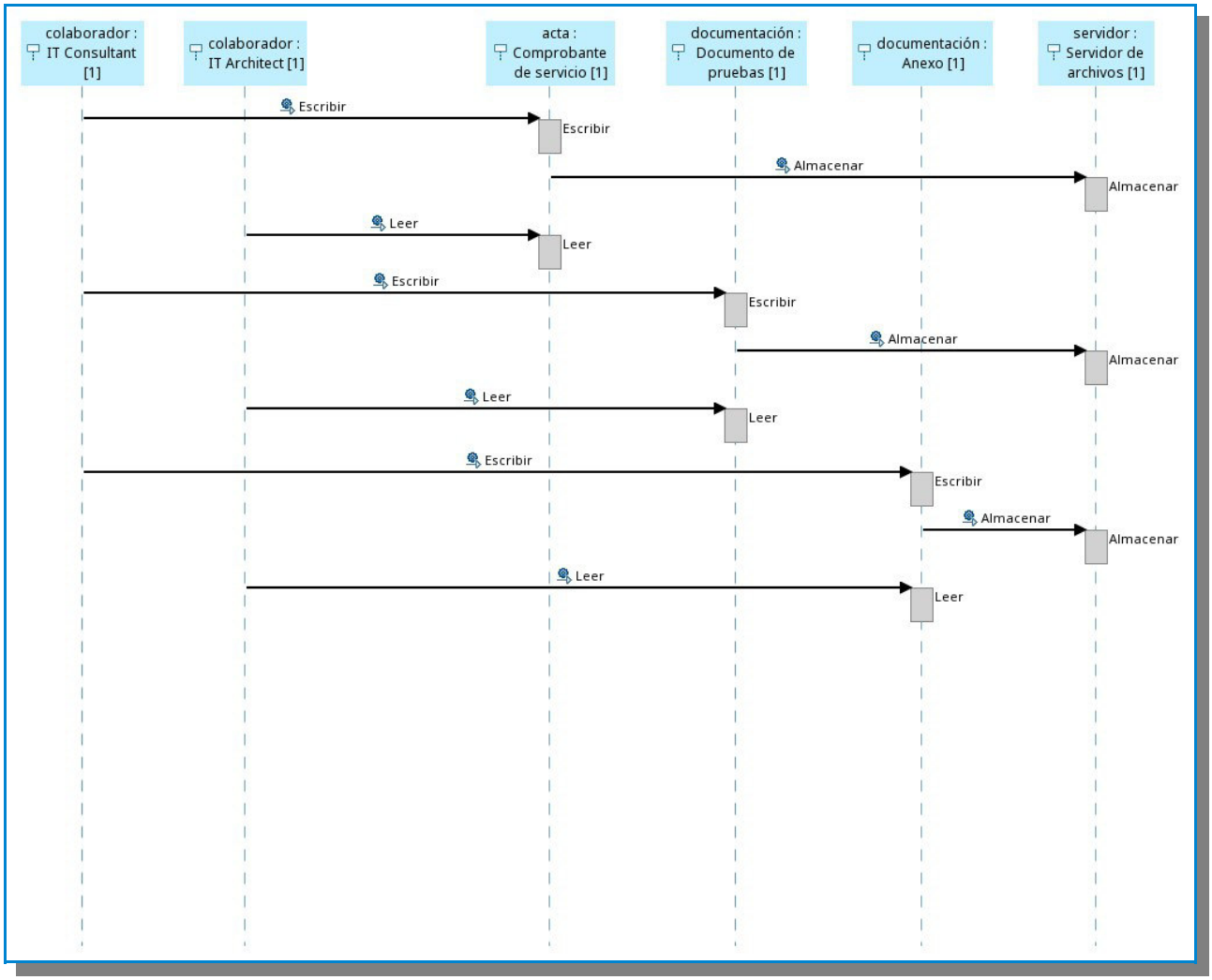


Figura 18: Diagrama de secuencia "Implementación"

Los conjuntos de objetos, métodos y permisos obtenidos son los siguientes:

- **Objetos:** “Comprobante de servicio”, “Documento de pruebas”, “Anexo”, “Servidor de archivos”.
- **Métodos:** “Escribir”, “Almacenar”, “Leer”.
- **Permisos:** (“Escribir”, “Comprobante de servicio”), (“Leer”, “Comprobante de servicio”), (“Escribir”, “Documento de pruebas”), (“Leer”, “Documento de pruebas”), (“Escribir”, “Anexo”), (“Leer”, “Anexo”), (“Almacenar”, “Servidor”).

- ***Puesta en producción***

  Este diagrama de secuencia representa el comportamiento de los actores hacia los objetos, dentro del caso de uso “Puesta en producción”. A partir de él, se puede obtener el conjunto de permisos asociados a los roles presentes en el modelo de control de acceso.

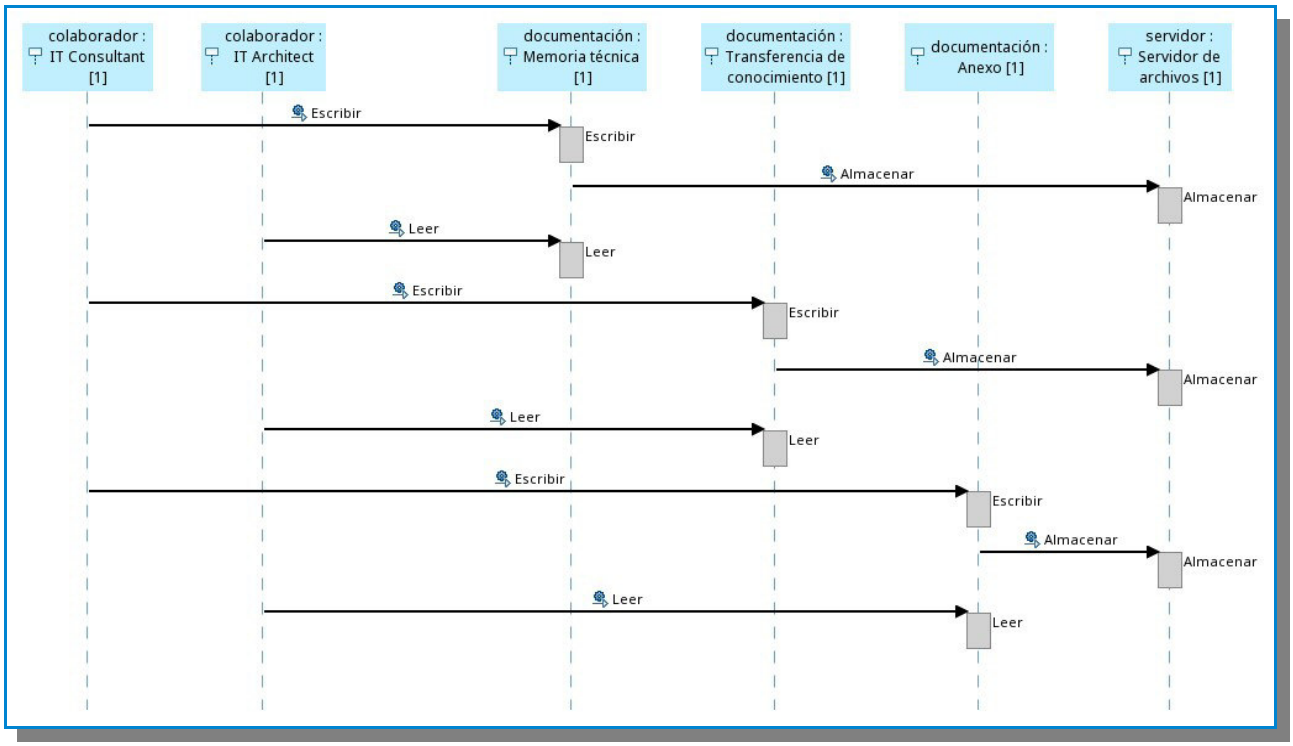


Figura 19: Diagrama de secuencia "Puesta en producción"

Los conjuntos de objetos, métodos y permisos obtenidos son los siguientes:

- **Objetos:** “Memoria técnica”, “Transferencia de conocimiento”, “Anexo”, “Servidor de archivos”.
- **Métodos:** “Escribir”, “Almacenar”, “Leer”.
- **Permisos:** (“Escribir”, “Memoria técnica”), (“Leer”, “Memoria técnica”), (“Escribir”, “Transferencia de conocimiento”), (“Leer”, “Transferencia de conocimiento”), (“Escribir”, “Anexo”), (“Leer”, “Anexo”), (“Almacenar”, “Servidor de archivos”).

## *1.3. Evaluación y selección del sistema*

### *1.3.1. Sistemas propuestos*

En base al estudio realizado en el *CAPÍTULO III. ESTADO DEL ARTE METODOLÓGICO*, se pudo identificar la presencia de dos sistemas de control de acceso que son básicamente los más representativos en el mercado y que podrían aplicarse para la resolución de nuestro problema. Estos sistemas de control de acceso son los siguientes:

- *Windows Server 2008 R2* con *Active Directory*.
- *Red Hat Enterprise Linux 7* con *Identity Management*.

A continuación pasaremos a desarrollar los criterios de selección para poder definir los puntos sobre los cuales seleccionaremos al sistema más adecuado para el desarrollo del presente proyecto.

### *1.3.2. Criterios de selección*

Para la selección del sistema de control de acceso, se tomara en cuenta los siguientes criterios: *crecimiento*, *control*, *costo*, *facilidad de gestión* y *facilidad de implementación*; los cuales definiremos a continuación:

- ***Control.-*** Relacionado a las limitaciones en el control de los sistemas Linux clientes.
- ***Crecimiento.-*** Relacionado al número de sistemas Linux que pueden ser gestionados por los responsables de sistemas.
- ***Costo.-*** Relacionado al coste en la implementación del sistema de control de acceso.
- ***Facilidad de gestión.-*** Relacionado a la facilidad en la gestión y configuración hacia los sistemas Linux clientes.
- ***Facilidad de implementación..-*** Relacionado a la facilidad en la implementación del sistema de control de acceso y la implementación del software requerido por los sistemas Linux clientes.

### *1.3.3. Análisis comparativo*

En esta sección se realizara un análisis comparativo entre los sistemas de control de acceso, tomando en cuenta los criterios de selección previamente establecidos y la información revisada ("Doing more with", 2014; “Informe Tecnológico, Red”, 2014) en la bibliografía.

| | Windows Server 2008 R2 con Active Directory | Re Hat Enterprise Linux 7 con Identity Management |
|---|---|---|
| **Control** | Se limita a proveer solo un punto de autenticación hacia los sistemas Linux. La gestión de los servicios se realiza de manera separada. | La infraestructura de Linux se incorpora a la infraestructura global de la empresa mediante relaciones de confianza con Active Directory. |
| **Crecimiento** | Los administradores pueden manejar un número limitado de sistemas Linux. | Se puede gestionar de forma centralizada miles de sistemas Linux. |
| **Costo** | Se necesita de la adquisición de licencias de uso por sistema, ademas de algún coste extra de software de terceros. | Sin ningún coste adicional. |
| **Facilidad de gestión** | Los sistemas Linux son gestionados por herramientas adicionales basadas en Windows. Así también se requiere la instalación de componentes adicionales y bastante esfuerzos para la configuración por sistema cliente. | Los sistemas Linux son gestionados por herramientas de Linux, sea por linea de comandos o una interface web de fácil uso. Así también se dispone de una sencilla utilidad para inscribirse en el sistema. |
| **Facilidad de implementación** | El sistema se despliegue desde el administrador de aplicaciones de Windows, a su vez el conjunto de software para los clientes se encuentra disponible desde su imagen de instalación y debe instalarse sistema por sistema. | Todos el software requerido para el despliegue del sistema y del utilitario cliente se encuentra disponible desde la imagen de instalación que puede ser usado como un único repositorio de software para el ambiente. |

En relación a a información expuesta en el análisis comparativo realizado, hemos optado en utilizar al sistema de *Red Hat Enteprise Linux 7* con *Identity Management* como base para el desarrollo de nuestra solución de sistema de control de acceso.

## *1.4. Aplicación del sistema*

### *1.4.1. Creación de servicios*

Dentro de la pestaña *Identity*, en la sección *Services*, presionar el botón *Add* para agregar un nuevo servicio dentro del sistema de control de acceso.

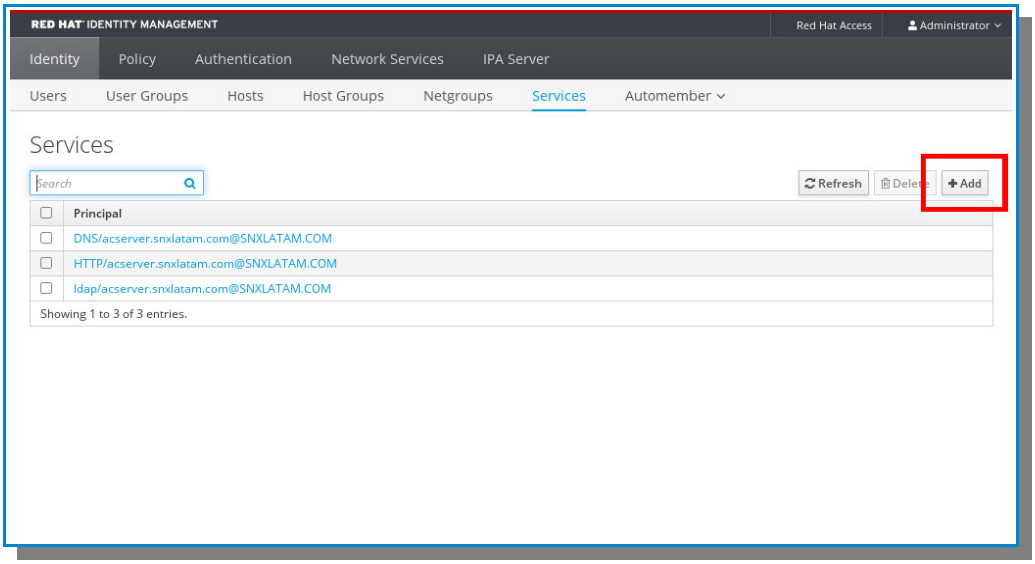


Figura 20: Adicionar nuevo servicio

Escribir el tipo del servicio en el campo *Service*, así también seleccionar el servidor cliente que ofrece dicho servicio. Presionar el botón *Add* para finalizar.

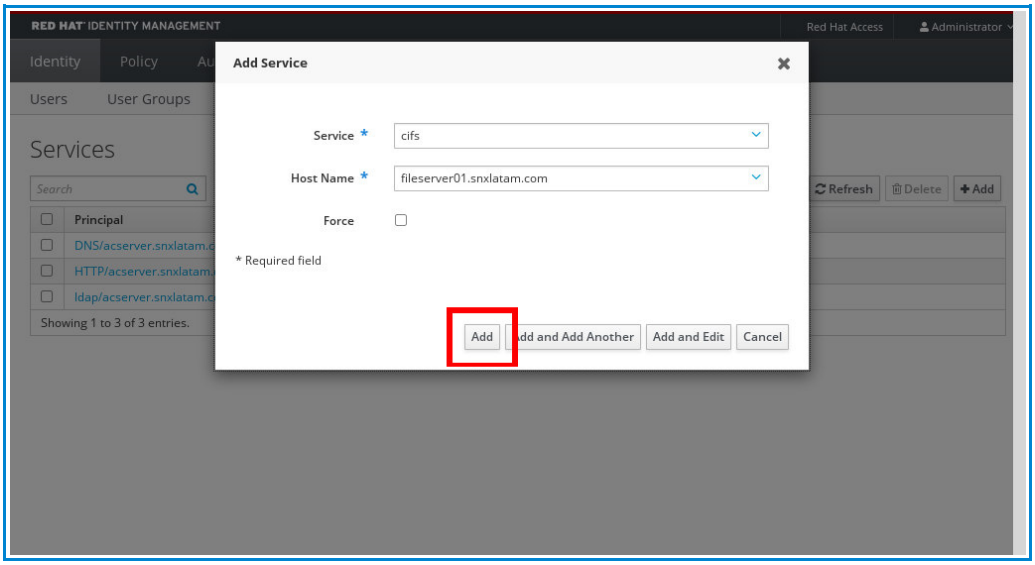


Figura 21: Finalizar la adición del servicio

Ejecutar la herramienta *ipa-getkeytab* desde un terminal para generar y asignar la nueva llave *keytab* al servicio principal.

```
[ root@server ~ ] # ipa-getkeytab -s acserver.snxlatam.com -p
cifs/fileserver01.snxlatam.com -k /etc/smb/krb5.keytab -e aes256-cts
```

Finalmente, se podrá visualizar las propiedades del servicio agregado en el *IPA Server* que se encuentra listo para ser aprovisionado o manipulado de manera remota.

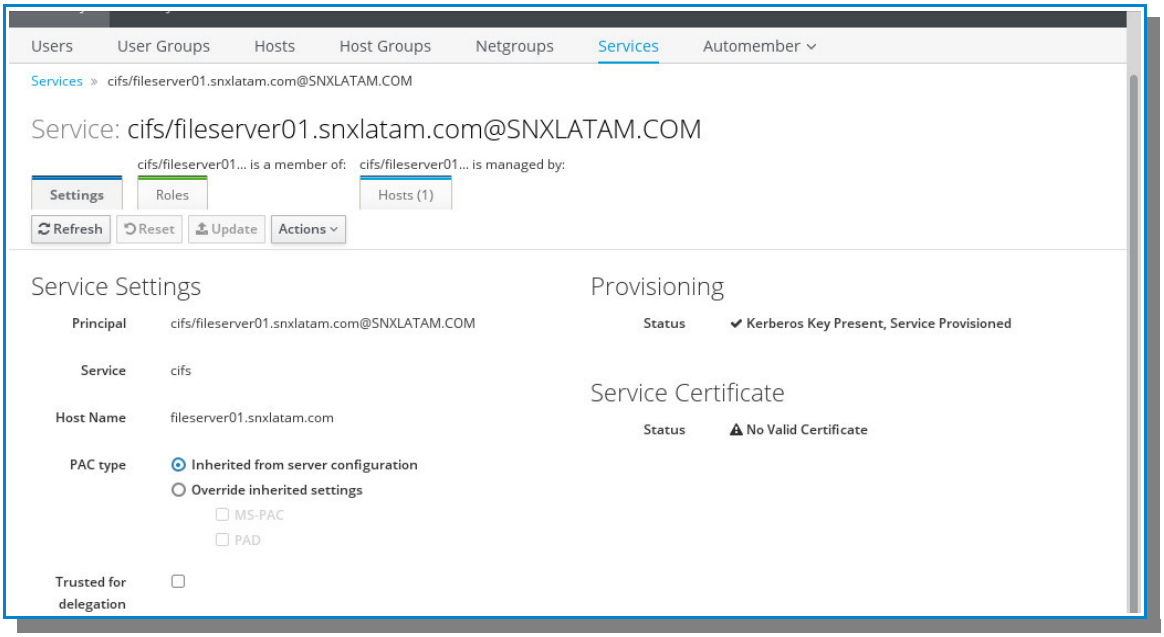

Figura 22: Propiedades del servicio

### *1.4.2. Creación de permisos*

Dentro de la pestaña *IPA Server*, seleccionar la opción de *Permissions* para ingresar al módulo de permisos.

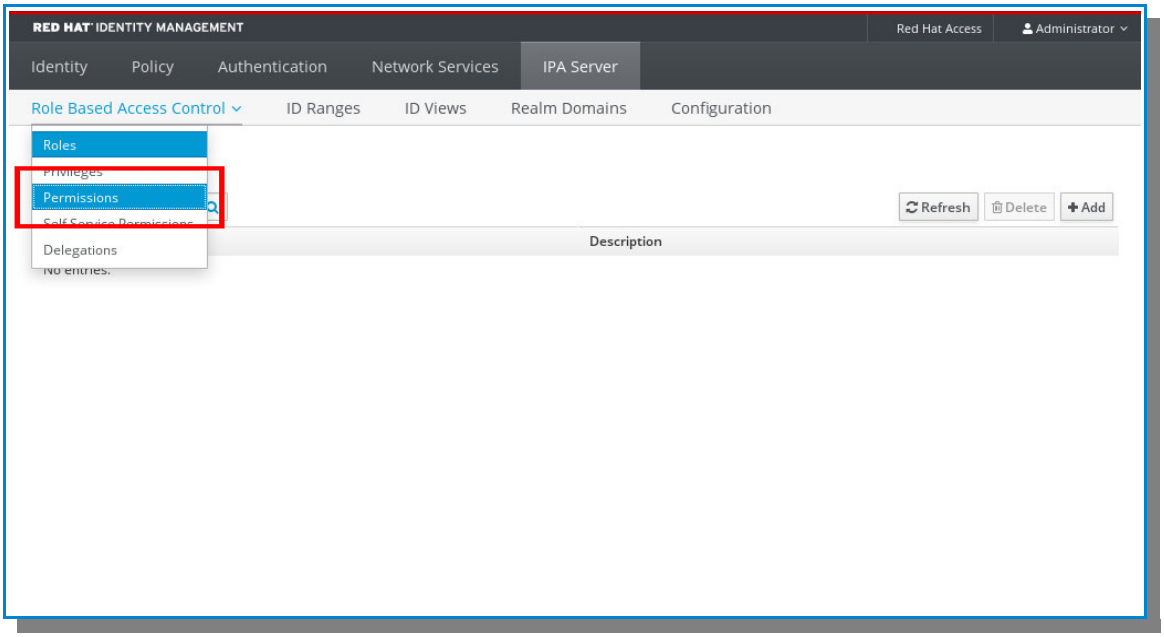


Figura 23: Acceder al módulo de permisos

Dentro del módulo de permisos, presionar el botón *Add* para agregar un nuevo permiso dentro del sistema de control de acceso.

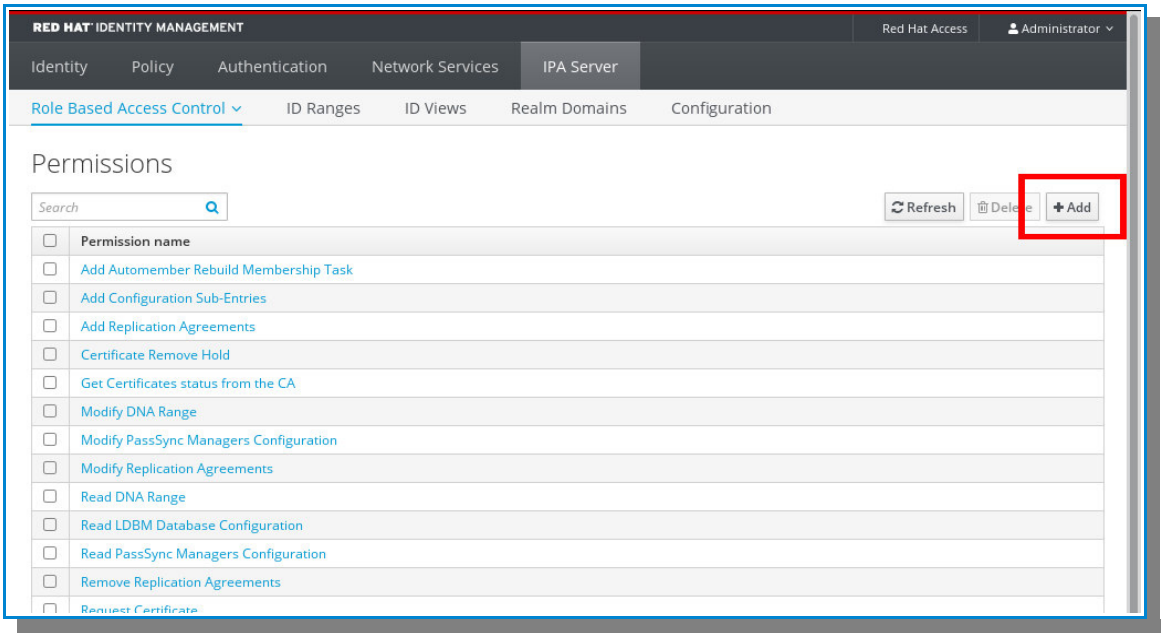


Figura 24: Agregar nuevo permiso

Escribir el nombre del permiso en el campo *Permission name,* y adjudicar algún tipo de permiso, se ya de lectura (*read*), escritura (*write*), ambos (*all*), entre otros. También escribir las propiedades del recursos que se encuentra registrado dentro del directorio de nuestro servidor de control de acceso para que se le pueda aplicar los permisos deseados. Finalmente, presionar el botón *Add* para finalizar.

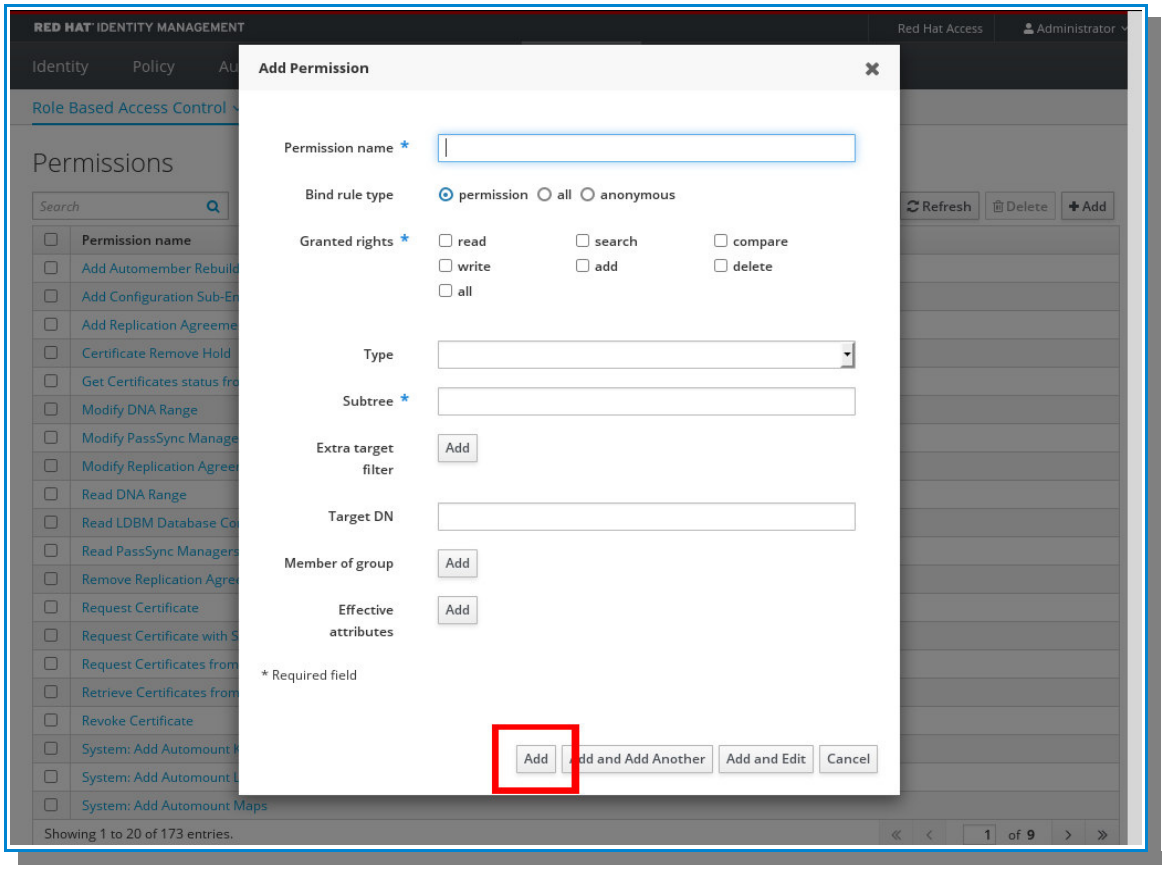


Figura 25: Finalizar la creación de permisos

Se procedió a crear los siguientes permisos en el sistema:

| Permisos de lectura | Permisos de lectura y escritura |
|---|---|
| Read directory Inicio del proyecto | Read Write directory Inicio del proyecto |
| Read directory Planificación del proyecto | Read Write directory Planificación del proyecto |
| Read directory Ejecución del proyecto | Read Write directory Ejecución del proyecto |
| Read directory Control de cambios | Read Write directory Control de cambios |
| Read directory Cierre del proyecto | Read Write directory Cierre del proyecto |
| Read directory Análisis del servicio | Read Write directory Análisis del servicio |
| Read directory Diseño de la arquitectura | Read Write directory Diseño de la arquitectura |
| Read directory Implementación | Read Write directory Implementación |
| Read directory Puesta en producción | Read Write directory Puesta en producción |

En la sección *Pemissions*, se podrá visualizar el nombre de los permisos creados. A través de este procedimiento, se procedió a crear el resto de los permisos definidos en los diagramas de secuencia relacionados al servicio de "Gestión de proyectos y consultoría"

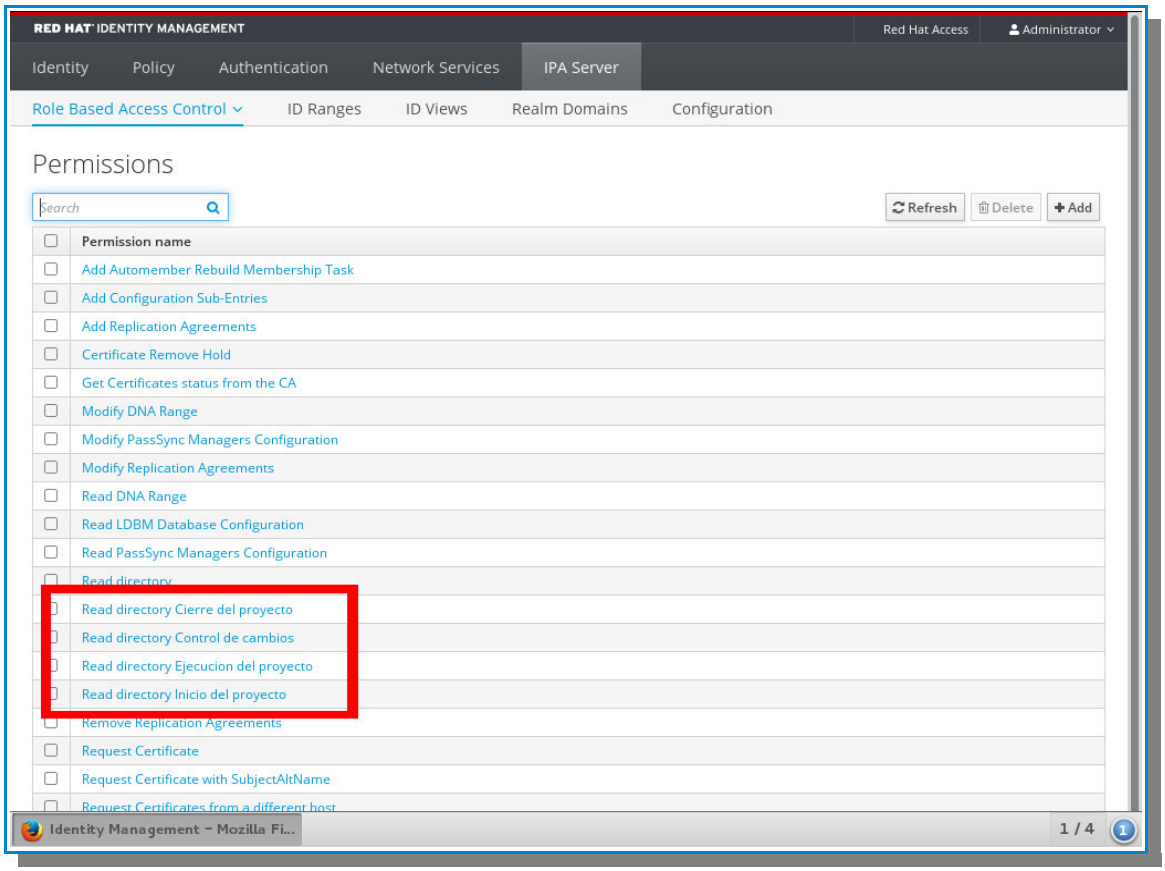


Figura 26: Relación de permisos creados

### *1.4.3. Creación de privilegios*

Dentro de la pestaña *IPA Server*, en la sección *Role Based Access Control*, seleccionar la opción de *Privileges* para acceder al módulo de privilegios.

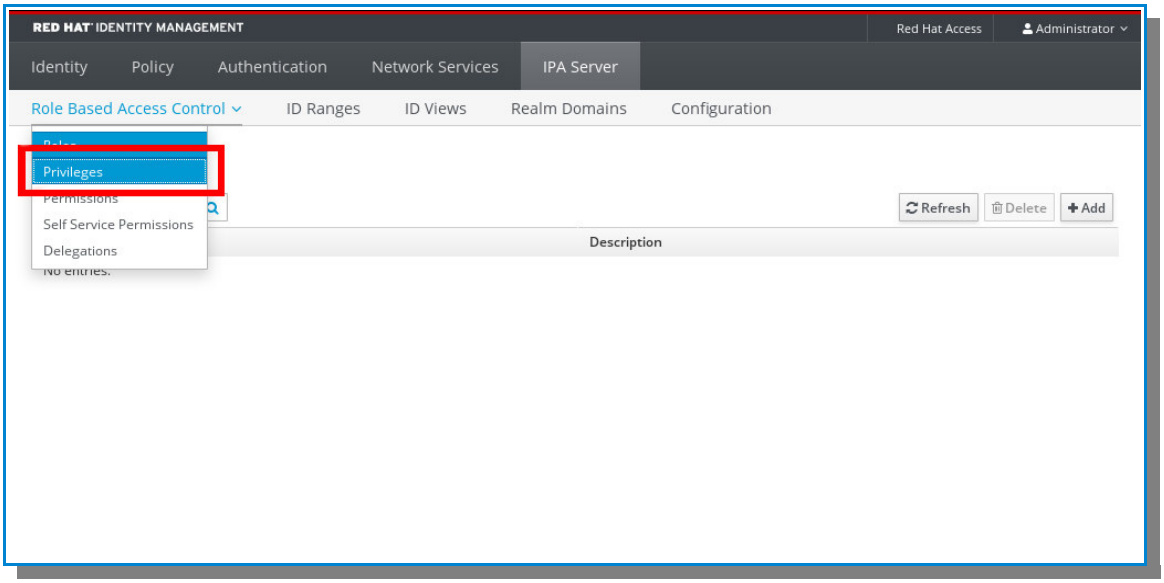


Figura 27: Acceder al módulo de privilegios

Dentro del módulo de privilegios, presionar el botón *Add* para agregar un nuevo privilegio dentro del sistema de control de acceso.

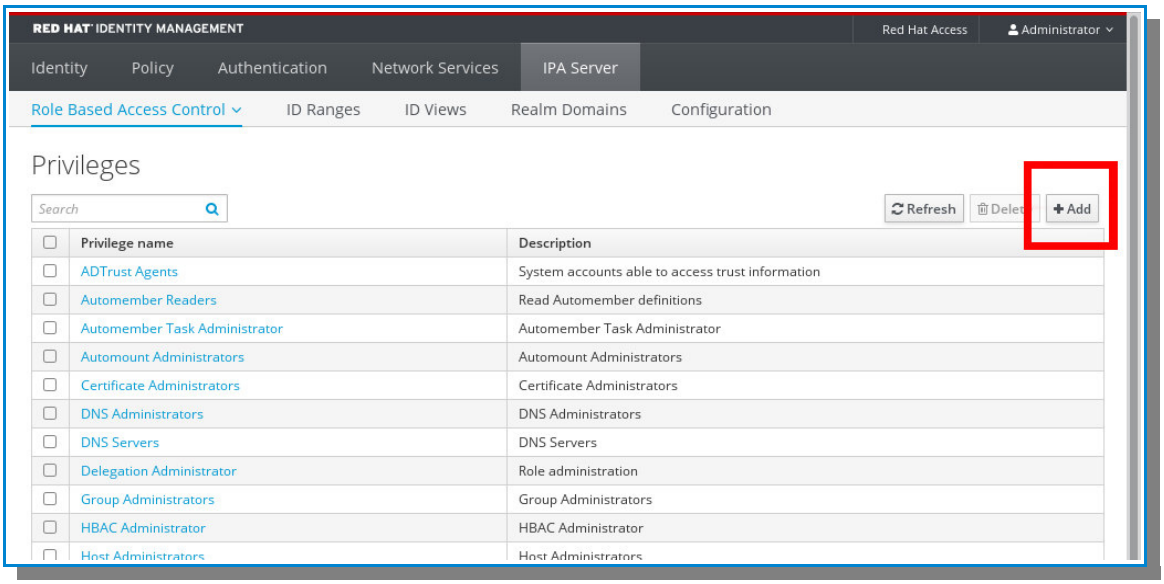


Figura 28: Agregar nuevo privilegio

Escribir el nombre del nuevo privilegio en el campo *Privilege name*, así también escribir la descripción del privilegio en el campo *Description*. Presionar el botón *Add* para finalizar.

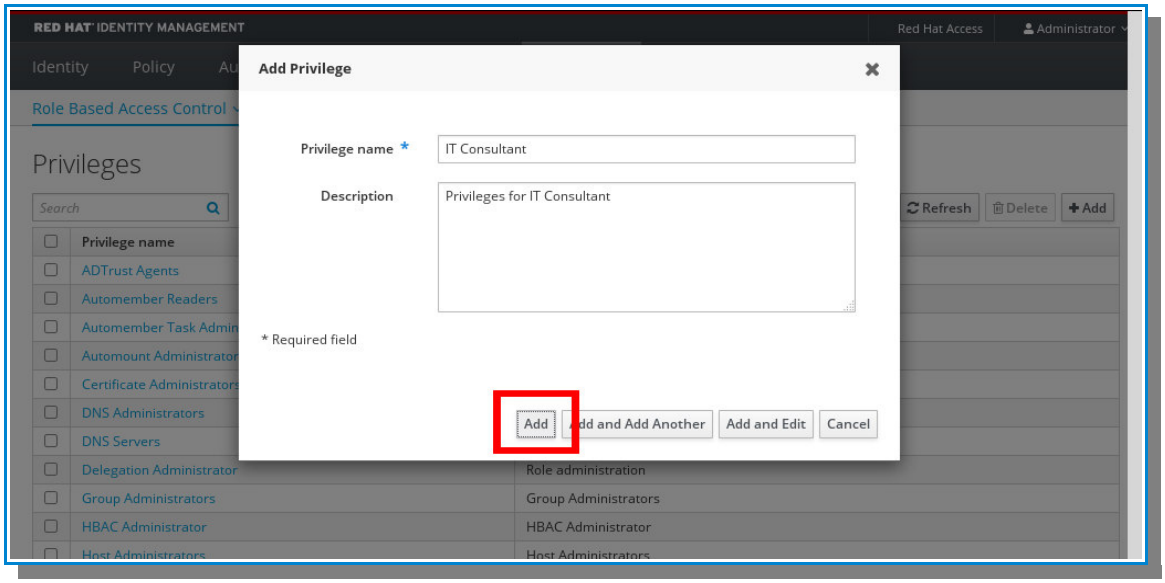


Figura 29: Finalizar la creación del privilegio

Ingresar a las propiedades del privilegio recientemente creado, haciendo click sobre el enlace que lo representa.

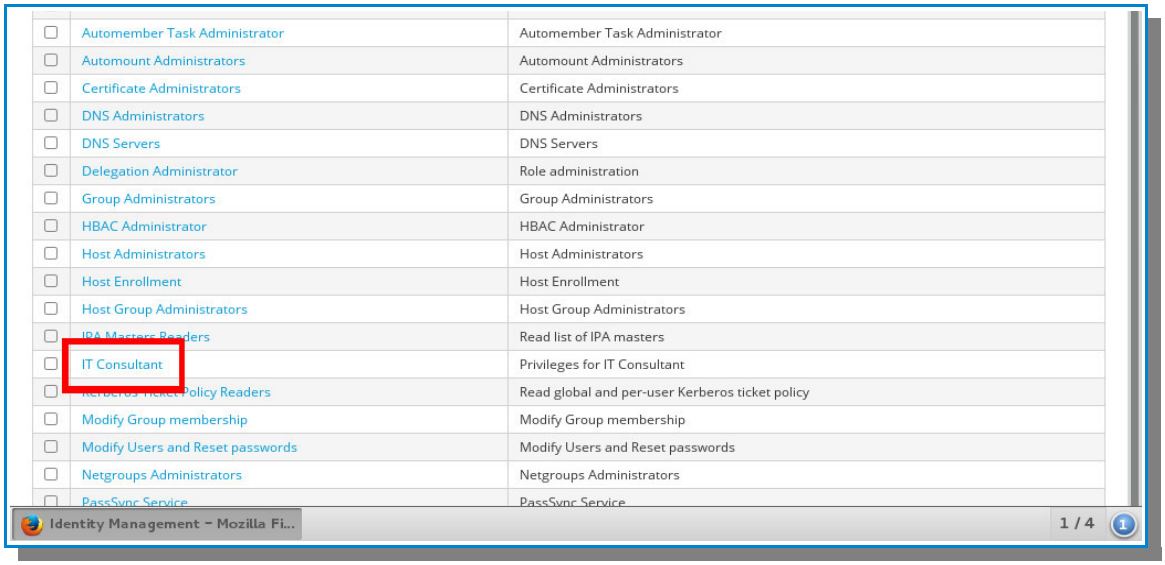


Figura 30: Ingresar a las propiedades del privilegio

Dentro de las propiedades del privilegio, en la sección *Permissions*, presionar el botón *Add* para asignar los permisos de lectura respectivos al privilegio.

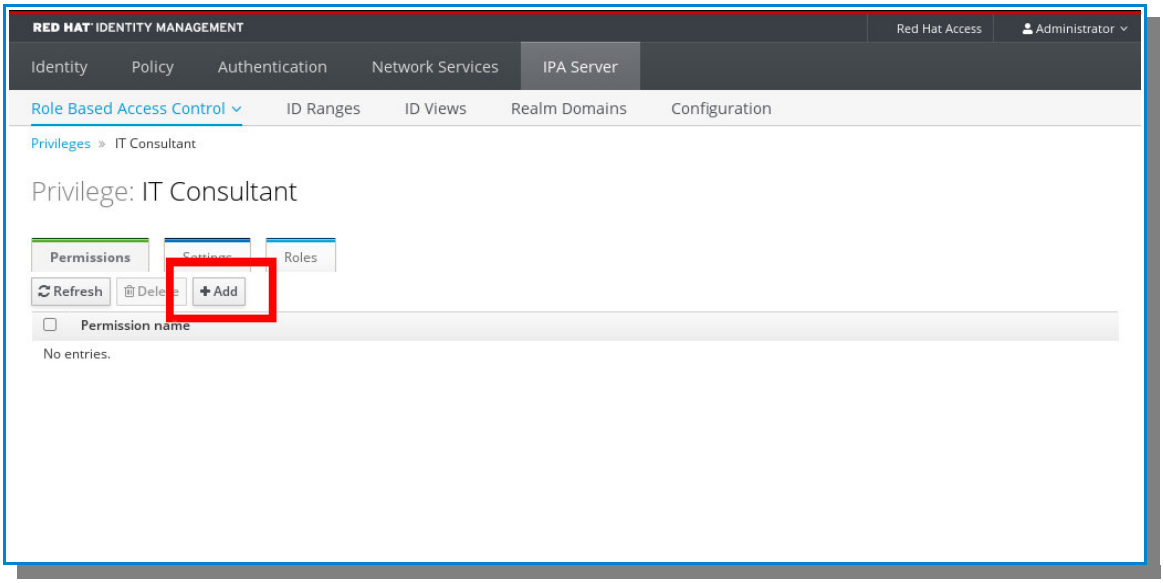


Figura 31: Asignar permisos de lectura al privilegio

Escribir *Read directory* en el campo *Filter*, para filtrar el listado de los permisos disponibles, luego seleccionar los permisos relacionados con el privilegio. Presionar el botón “>” para asociarlos.

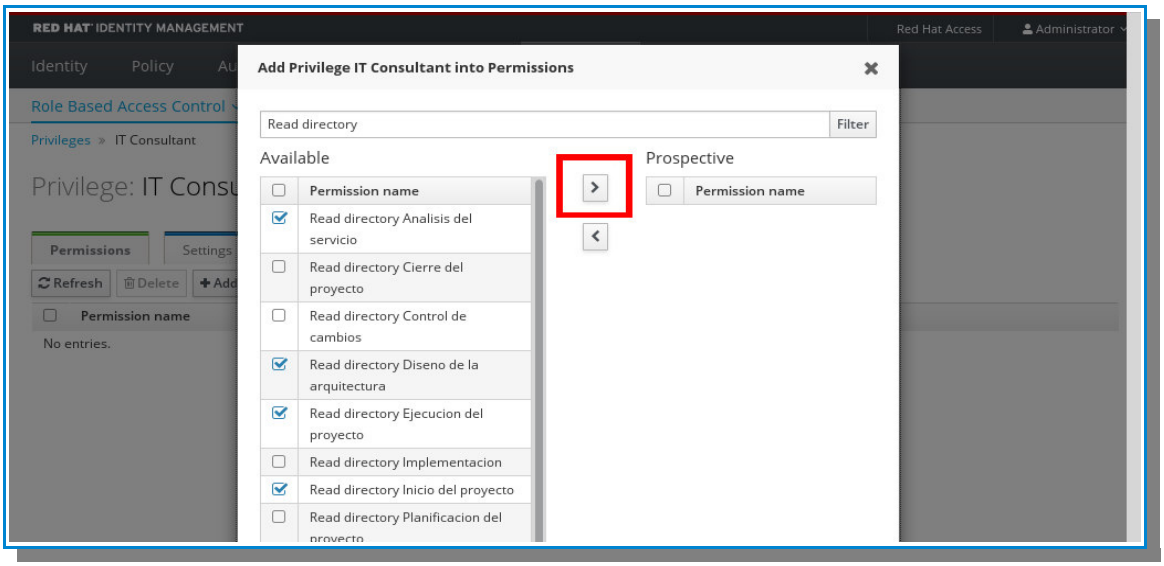


Figura 32: Seleccionar permisos de lectura

Una vez asociados los permisos al privilegio, presionar el botón *Add* para finalizar.

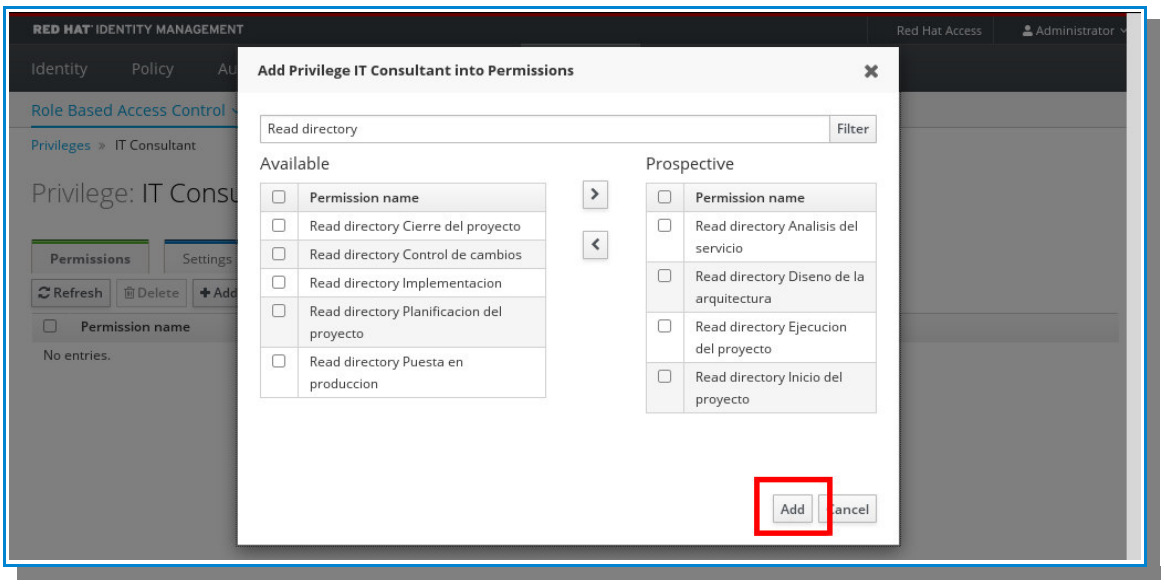


Figura 33: Finalizar la asignación de permisos de lectura

Dentro de las propiedades del privilegio nuevamente, en la sección *Permissions*, presionar el botón *Add* para asignar los permisos de lectura/escritura respectivos al privilegio.

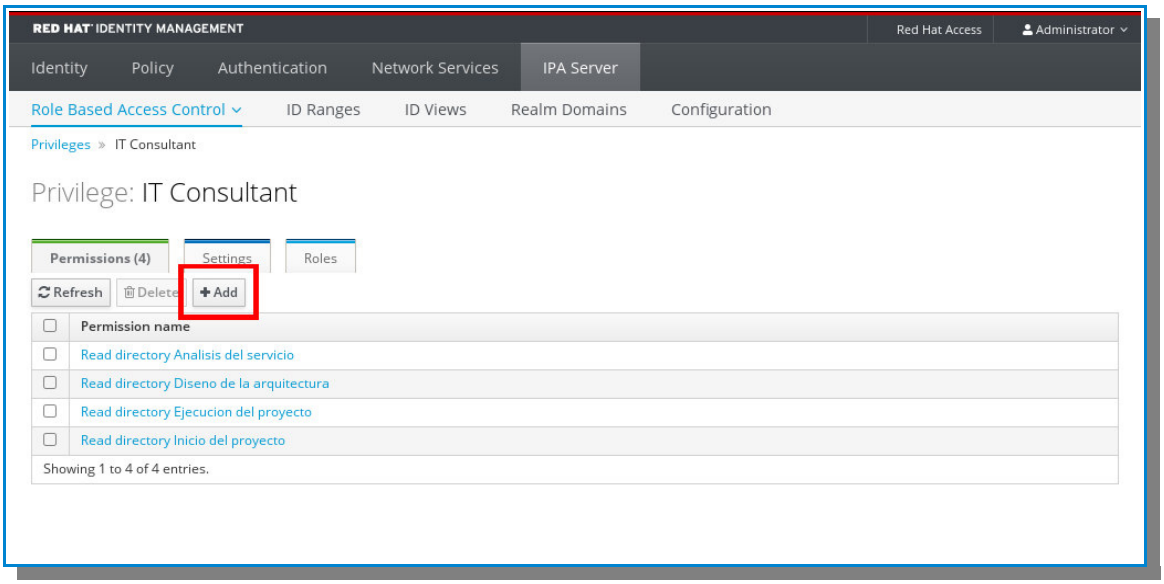


Figura 34: Asignar permisos de lectura/escritura al privilegio

Escribir *Read Write* en el campo *Filter*, para filtrar el listado de los permisos disponibles, luego seleccionar los permisos relacionados con el privilegio. Presionar el botón ">" para asociarlos.

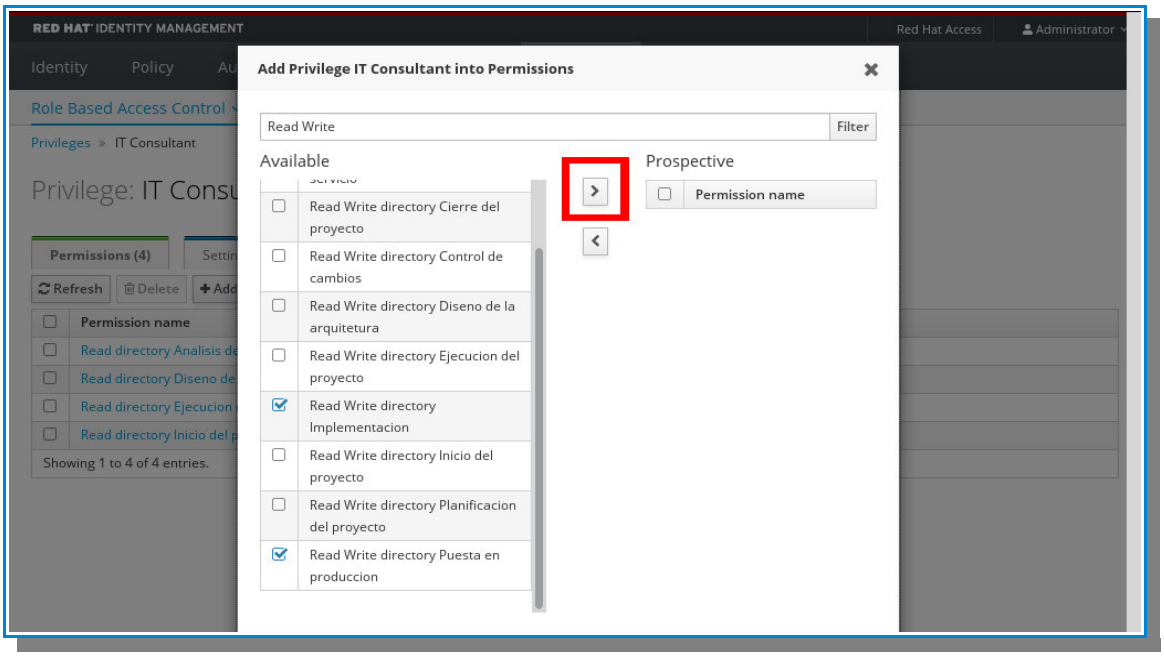


Figura 35: Seleccionar permisos de lectura/escritura

Una vez asociados los permisos al privilegio, presionar el botón *Add* para finalizar.

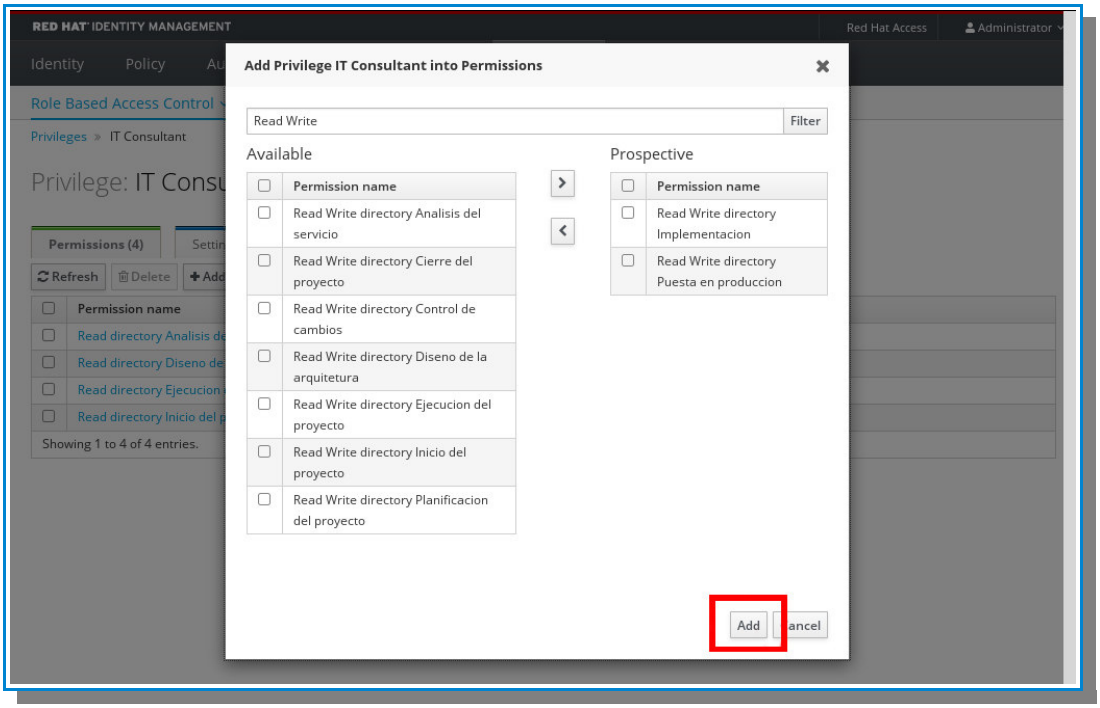


Figura 36: Finalizar la asignación de permisos de lectura/escritura

En la sección *Pemissions*, se podrá visualizar el nombre de los permisos asociados a un privilegio en particular.

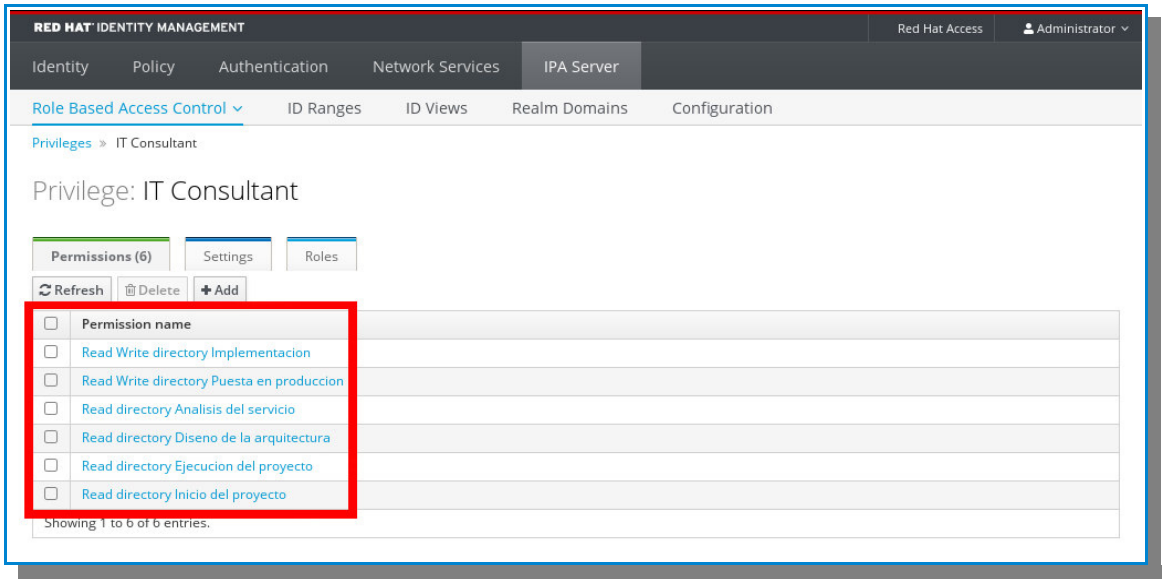


Figura 37: Relación de permisos asociados al privilegio

A través de este procedimiento, se procedió a crear el resto de los privilegios definidos en los diagramas de secuencia relacionados al servicio de "Gestión de proyectos y consultoría"

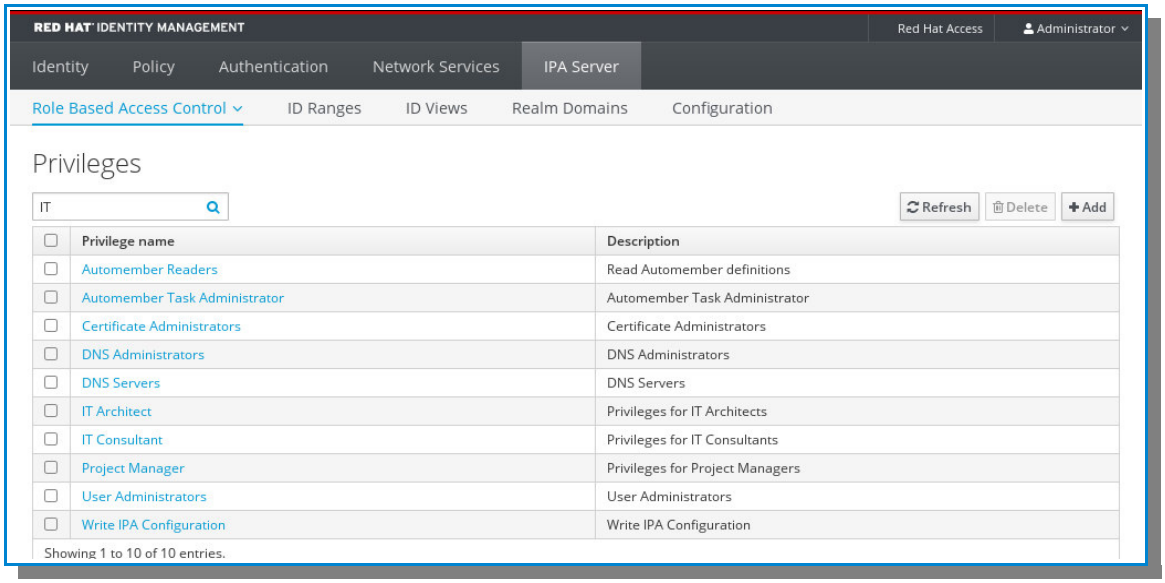


Figura 38: Lista de privilegios creados

### *1.4.4. Creación de roles*

Dentro de la pestaña *IPA Server*, en la sección *Role Based Access Control*, seleccionar la opción de *Roles* para acceder al módulo de roles.

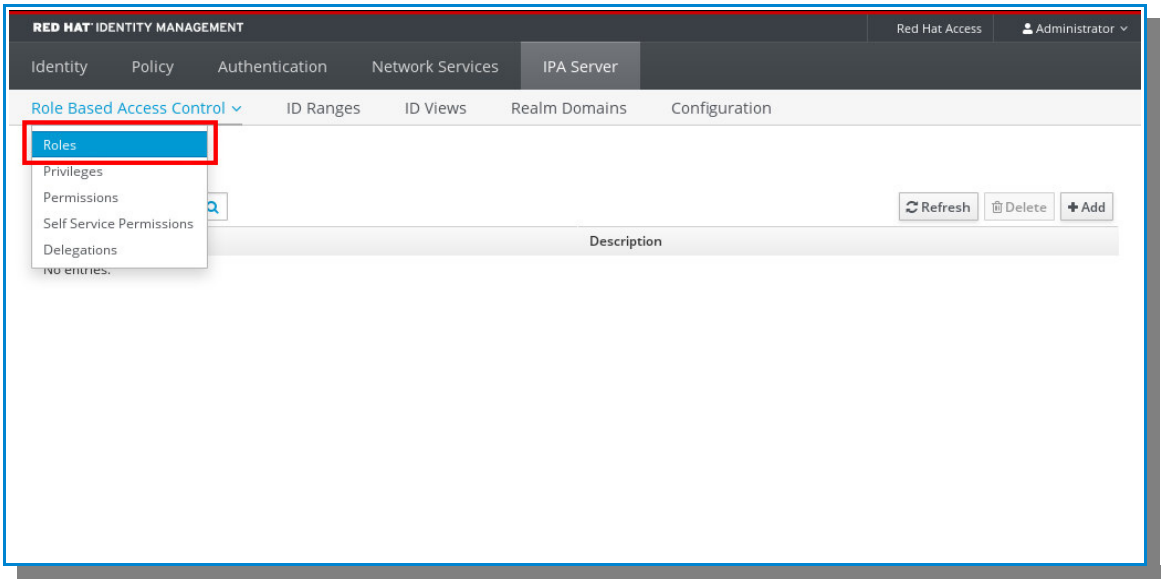


Figura 39: Acceder al módulo de roles

Dentro del módulo de roles, presionar el botón *Add* para agregar un nuevo rol dentro del sistema de control de acceso.

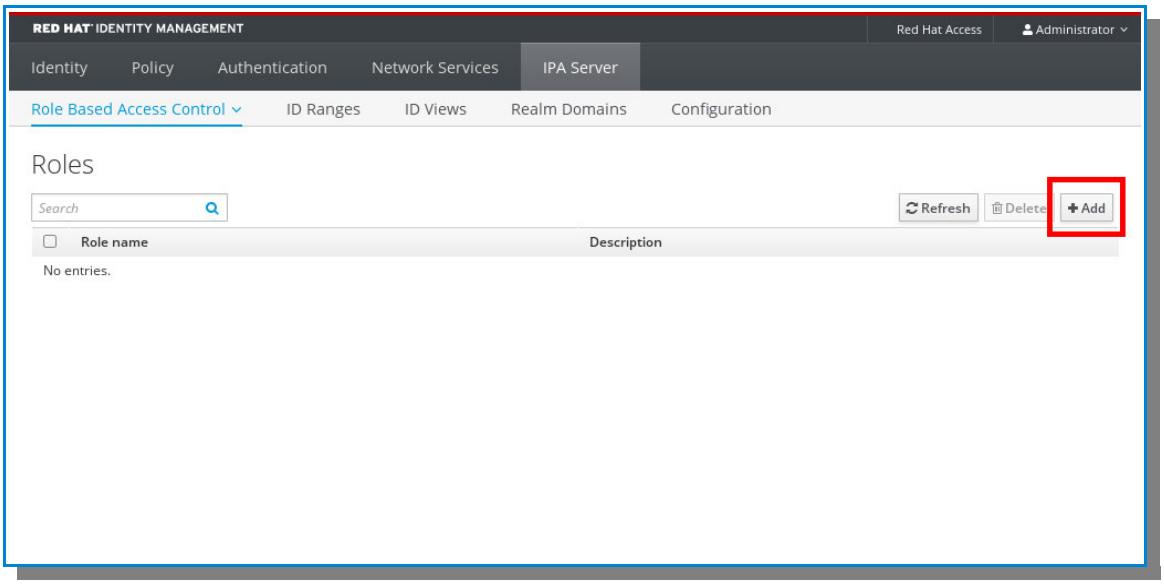


Figura 40: Agregar nuevo rol

Escribir el nombre del nuevo rol en el campo *Role name*, así también escribir la descripción del rol en el campo *Description*. Presionar el botón *Add* para finalizar.

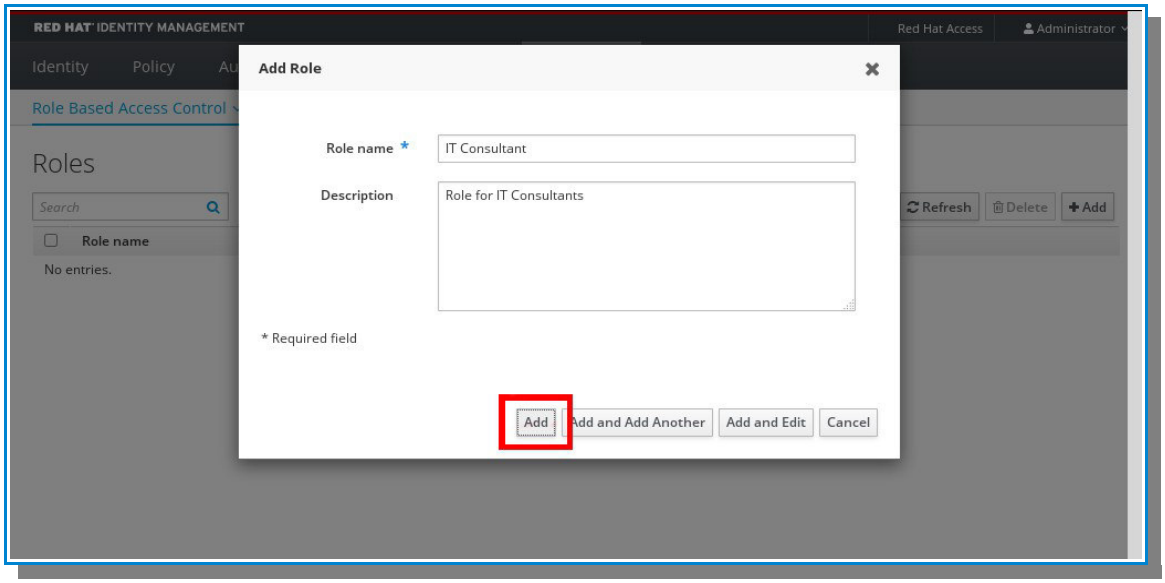


Figura 41: Finalizar la creación del rol

Ingresar a las propiedades del rol recientemente creado, haciendo click sobre el enlace que lo representa.

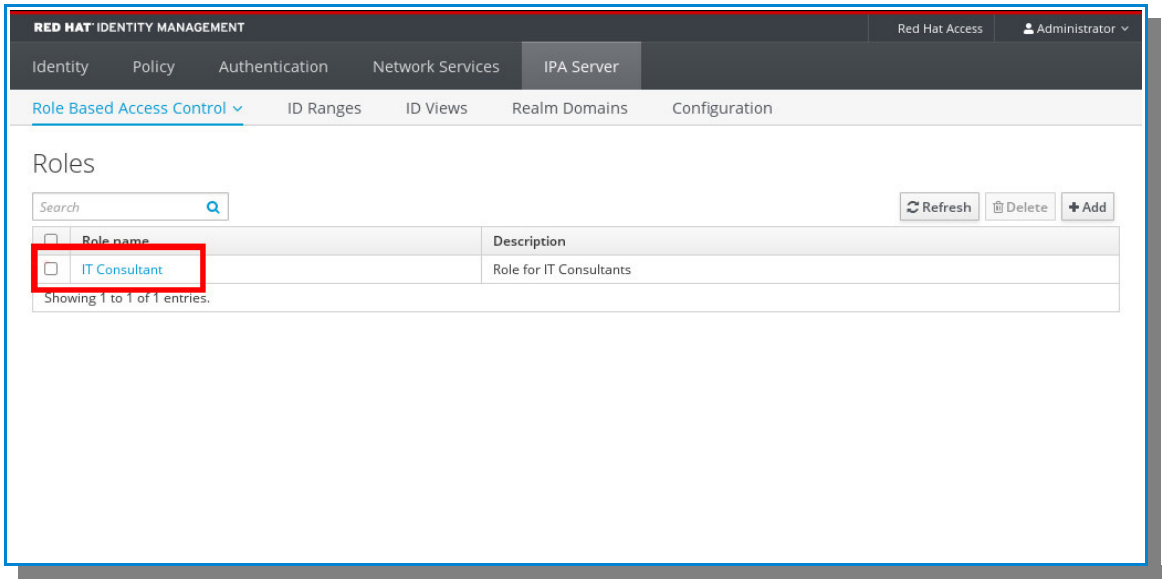


Figura 42: Ingresar a las propiedades del rol

Dentro de las propiedades del rol, en la sección *Privileges,* presionar el botón *Add* para asignar los privilegios respectivos al rol.

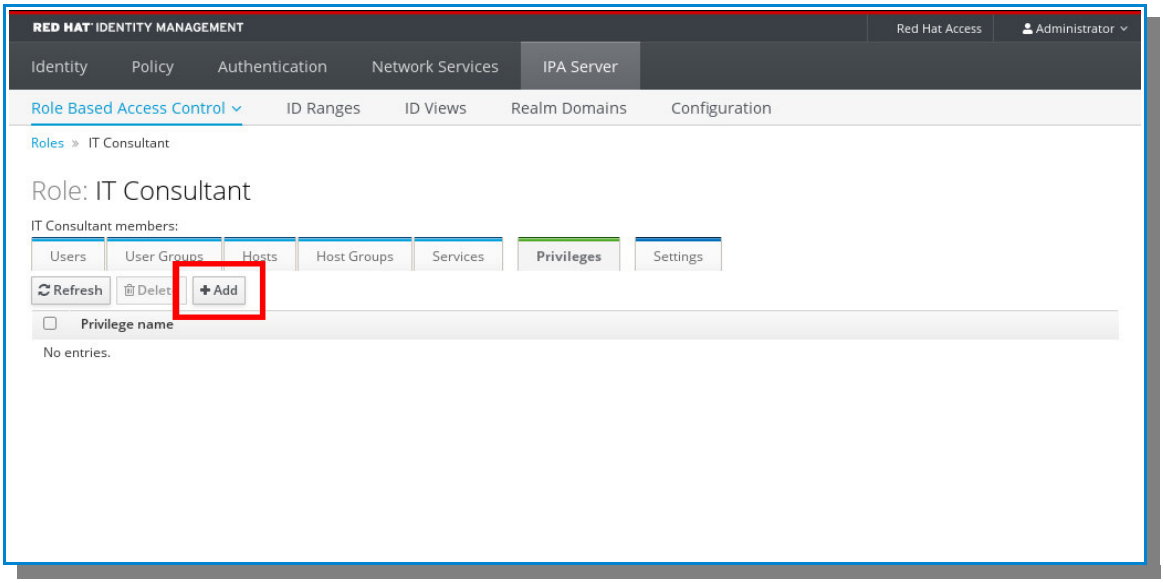


Figura 43: Asignar privilegios al rol

Escribir el nombre del privilegio en el campo *Filter*, para filtrar el listado de los privilegios disponibles, luego seleccionar el privilegio relacionado con el rol. Presionar el botón ">" para asociarlo.

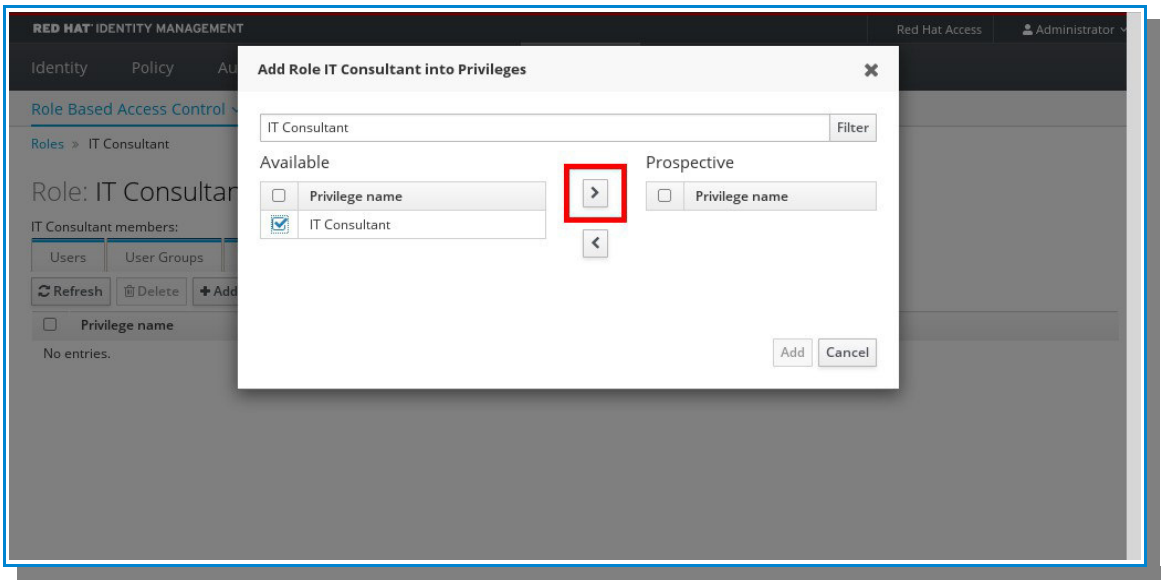


Figura 44: Seleccionar privilegios

Una vez asociado el privilegio al rol, presionar el botón *Add* para finalizar.

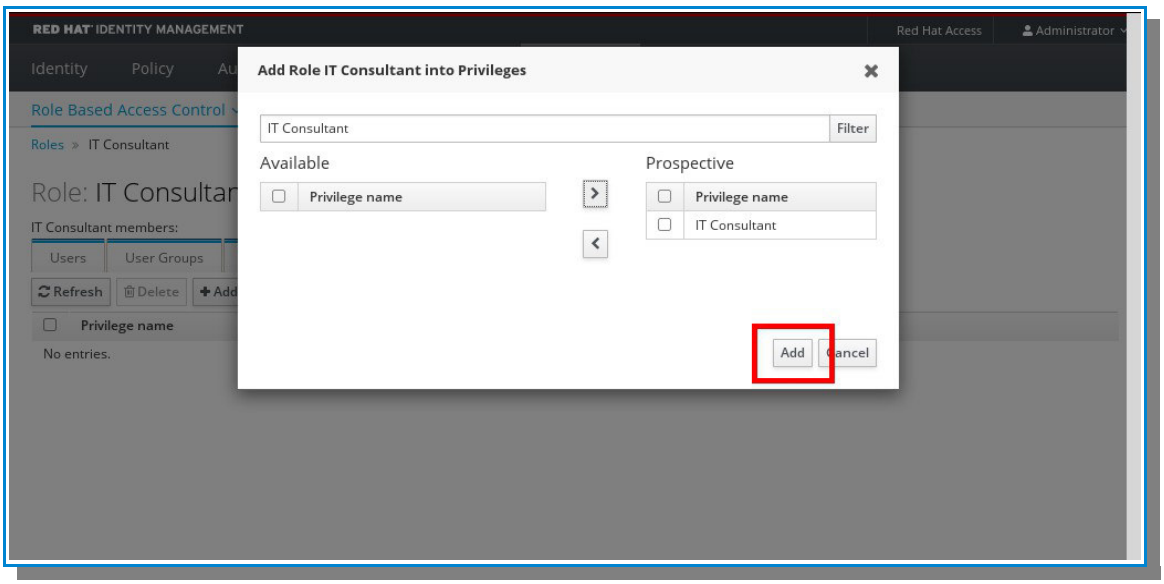


Figura 45: Finalizar la asignación de privilegios

En la sección *Privileges*, se podrá visualizar el nombre del privilegio asociado a un rol en particular.

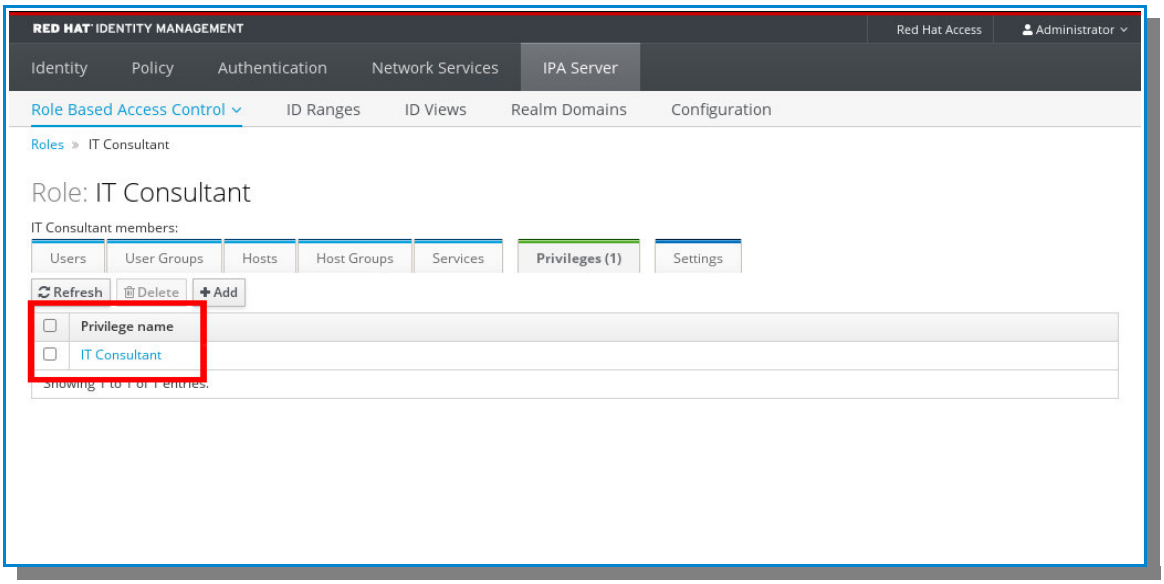


Figura 46: Relación de privilegios asociados al rol

A través de este procedimiento, se procedió a crear el resto de los roles definidos en los diagramas de casos de uso relacionados al servicio de “Gestión de proyectos y consultoría”.

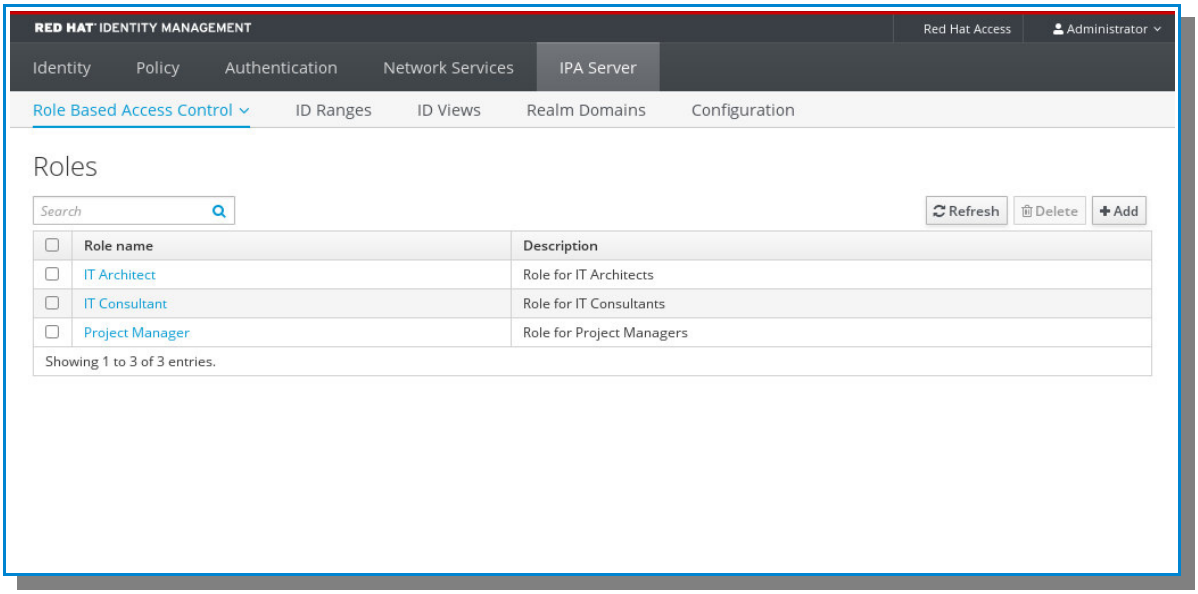


Figura 47: Lista de roles creados

### *1.4.5. Creación de usuarios*

Dentro de la pestaña *Identity*, en la sección *Users*, presionar el botón *Add* para agregar un nuevo usuario dentro del sistema de control de acceso.

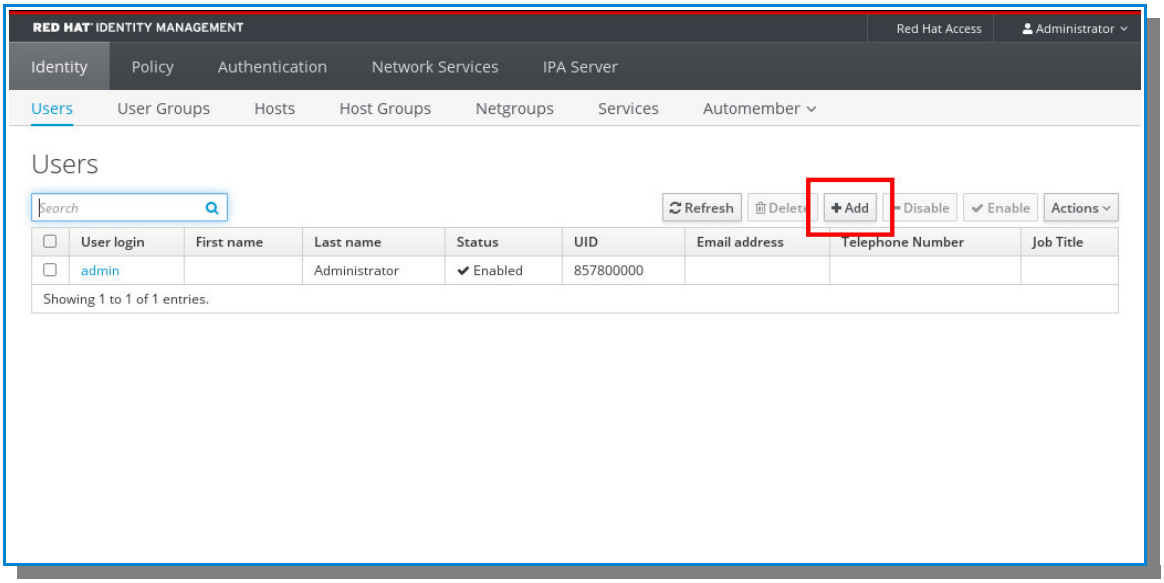


Figura 48: Agregar nuevo usuario

Escribir el nombre del nuevo usuario en el campo *User login*, así también escribir el nombre y apellido de la persona relacionada a dicho usuario en los campos *First name* y *Last name* respectivamente. Presionar el botón *Add* para finalizar

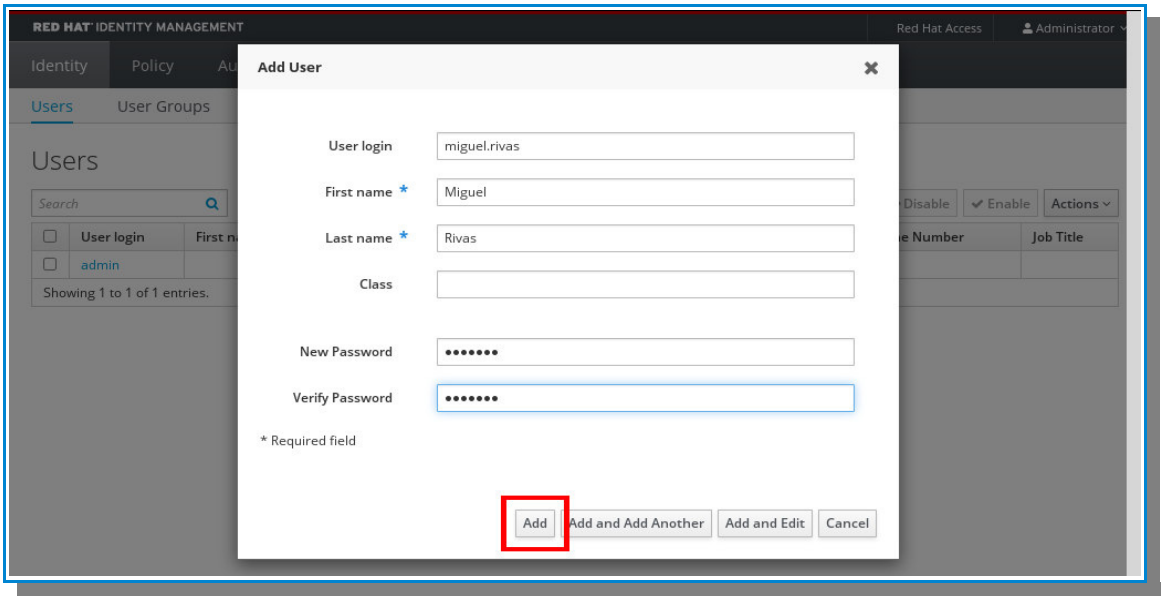


Figura 49: Finalizar la creación del usuario

Ingresar a las propiedades del usuario recientemente creado, haciendo click sobre el enlace que lo representa.

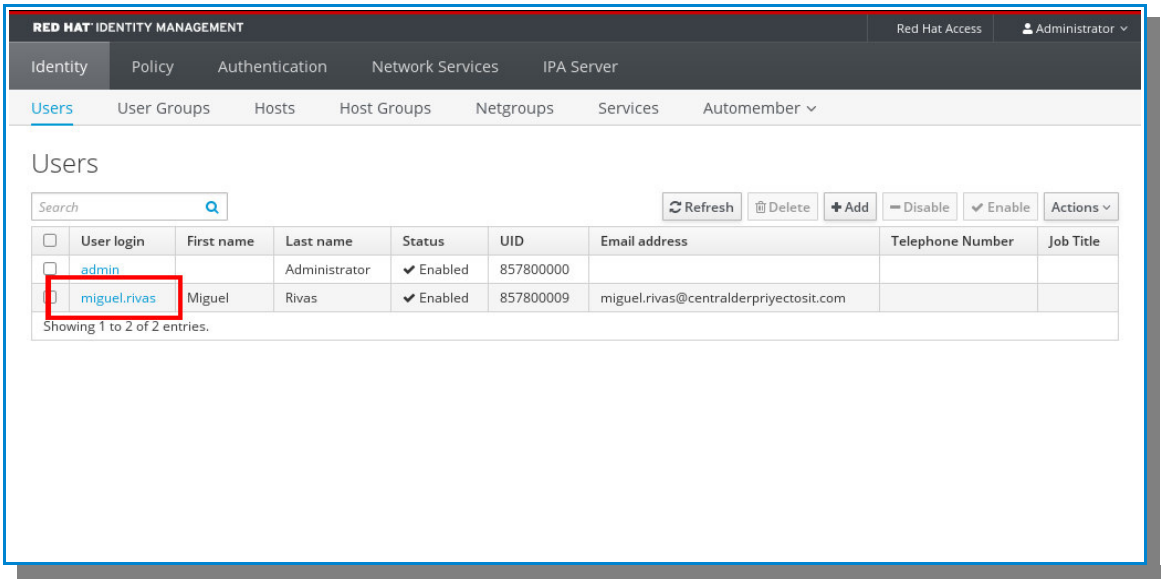


Figura 50: Ingresar a las propiedades del usuario

Dentro de las propiedades del usuario, en la sección *Roles*, presionar el botón *Add* para asignar el rol respectivo a dicho usuario.

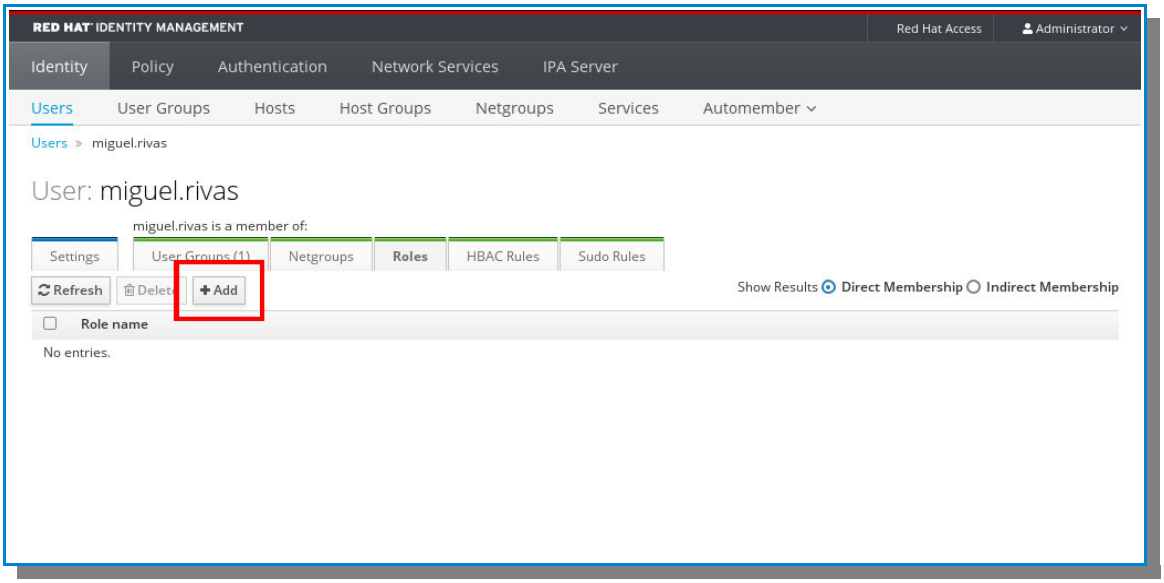


Figura 51: Asignar rol al usuario

Seleccionar el rol que sera relacionado con el usuario. Presionar el botón “>” para asociarlo.

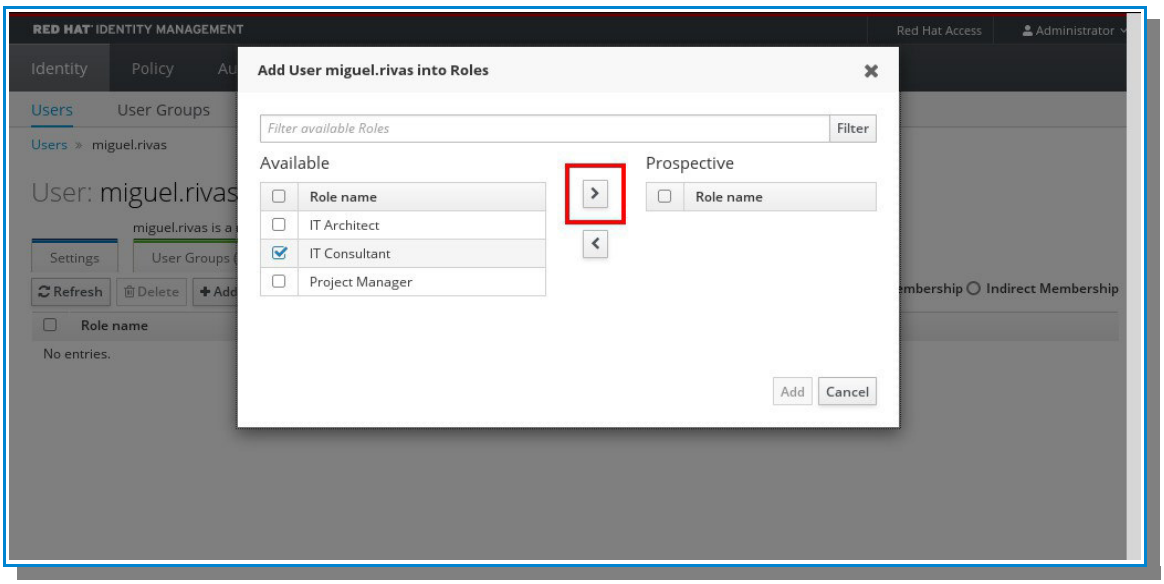


Figura 52: Seleccionar rol

Una vez asociado el rol al usuario, presionar el botón *Add* para finalizar.

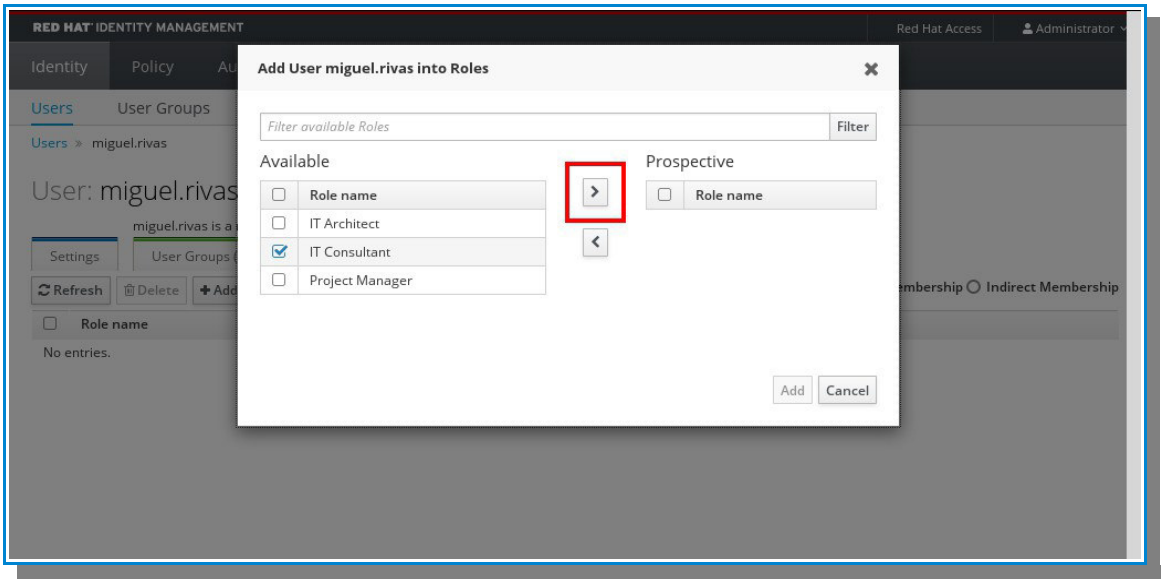


Figura 53: Finalizar la asignación de roles

En la sección *Roles*, se podrá visualizar el nombre de los roles asociados a un usuario en particular.

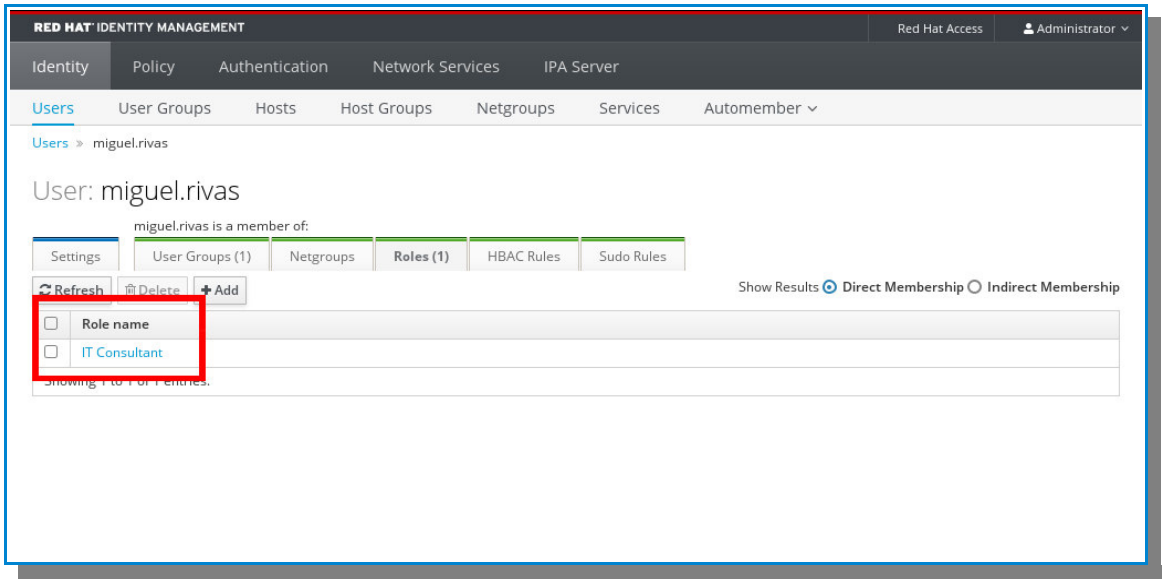


Figura 54: Relación de roles asociados al usuario

A través de este procedimiento, se procedió a crear al resto de los usuarios de la empresa que participan dentro del servicio de "Gestión de proyectos y consultoría".

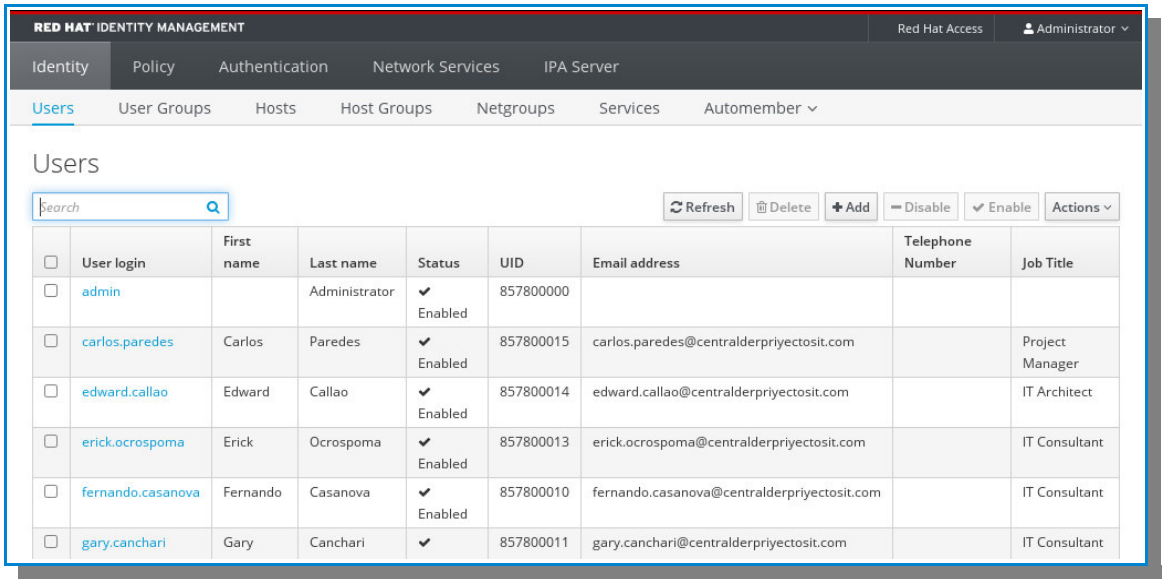


Figura 55: Lista de usuarios creados

## 2. Descripción de la solución tecnológica

A continuación pasaremos a describir la topología, en donde se muestra las interacciones que existen entre el sistema de control de acceso con el restos de servidores involucrados en el ambiente. Así también mostraremos lo requerimientos mínimos que fueron tomados en cuenta para el despliegue de nuestra solución.

### *2.1. Arquitectura de la solución*

El sistema de control de acceso desplegado sobre un servidor *Red Hat Enterprise Linux 7*, establece una comunicación con los servidores de archivos principalmente a través del protocolo *SSSD*. Con esta relación, el sistema de control de acceso también puede ofrecer los servicios de los servidores de archivos y les aplica los permisos establecidos anteriormente

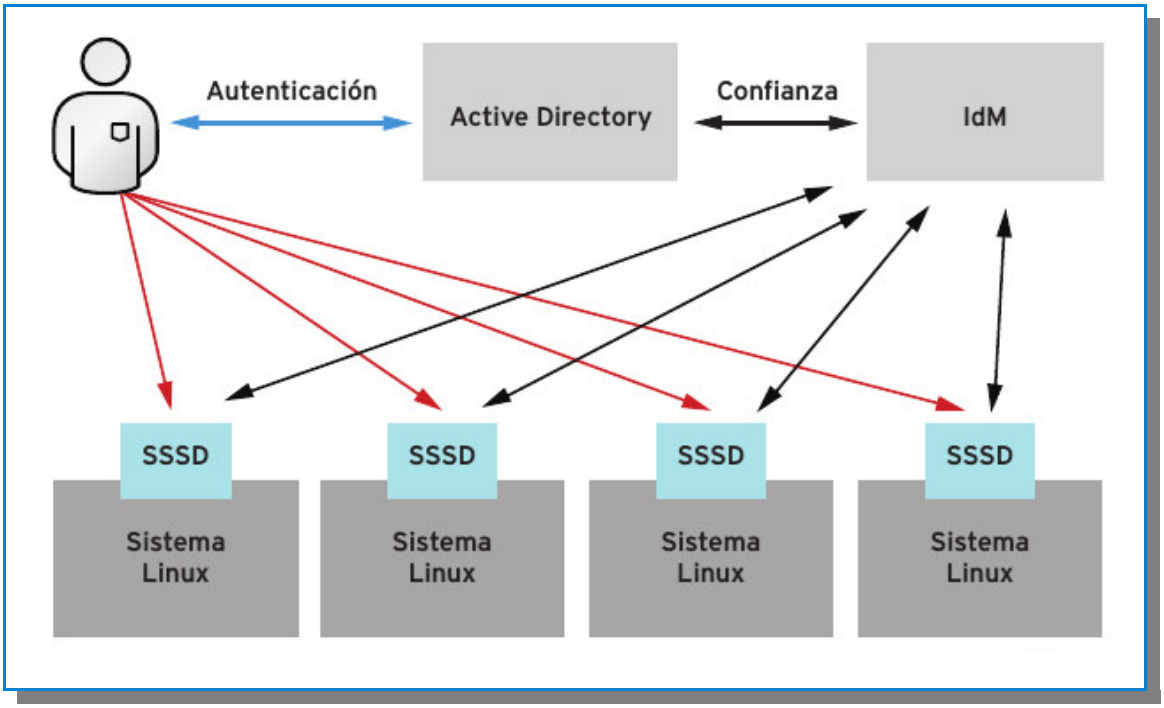


Figura 56: Arquitectura de la solución

Adicionalmente, se establece una relación de confianza entre directorio activo de la empresa y el sistema de control de acceso, para que los usuarios dentro de la red *Windows* (usuarios que también fueron creados en el sistema de control de acceso) puedan hacer uso de dichos recursos disponibles en los servidores de archivos; pero ahora a través del sistema de control de acceso; de acuerdo a los permisos entablados.

## *2.2. Requerimientos mínimos*

La instalación del sistema de control de acceso y su configuración requiere que se cumplan con ciertos requisitos como mínimo para su correcto funcionamiento sobre el entorno que se desee desplegar:

### *2.2.1. Requerimientos de hardware*

- La solución de sistema de control de acceso se desplegó sobre un servidor virtual que contaba con las siguientes características mínimas:

| | |
|---|---|
| Memoria RAM | 3 GB |
| Procesadores | 4 cores |
| Disco duro | 20 GB |
| Interfaces de red | 1 NIC 100/1000T |

### *2.2.2. Requerimientos de software*

- Esta solución de sistema de control de acceso trabaja sobre una plataforma *Red Hat Enterprise Linux 7*, y utiliza software necesario para su instalación (software principal y dependencias) pueden ser sustraídos desde la media a través de un repositorio local o remoto.

### *2.2.3. Requerimientos adicionales*

- Registro y conexiones al servidor *DNS* de la organización para garantizar la resolución de nombres de los servidores.
- Permitir la comunicación entre los servidores clientes y el servidor que desempeña las funciones de sistema de control de acceso, al menos por los siguientes puertos *TCP/IP* inicialmente:

| Servicio | Puerto | Tipo |
|---|---|---|
| LDAP/LDAPS | 389,636 | TCP |
| Kerberos | 88,464 | TCP |
| DNS | 53 | TCP y UDP |

# CAPÍTULO V. CONCLUSIONES Y RECOMENDACIONES

## 1. Conclusiones

- La estructuración de un modelo de control de acceso basado en roles es una tarea demasiado laboriosa, pero detalla con exactitud cuales son los requerimientos de acceso a la información que tiene los actores de un servicio en particular.
- La implementación y gestión del sistema de control de acceso bajo plataforma *Linux*, resulta no tener mayor complejidad ya que el software requerido para su despliegue es mínimo y aplica las configuraciones necesarias en los clientes de manera automática.
- Finalmente, podemos concluir que un sistema de control de acceso desarrollado sobre plataforma *Linux*, es una opción muy adecuada cuando se quiere integrar los recursos del resto de servicios *Linux* a la red de usuarios, de una manera practica y sencilla.

## 2. Recomendaciones

- Se recomienda que se pueda efectuar este mismo mecanismo, con el fin de integrar más servicios desplegados sobre plataforma *Linux* o *Unix*, a una red de *Microsoft* que cuente con *Active Directory* desplegados en sus versiones más actuales.

## REFERENCIAS BIBLIOGRÁFICAS

### 1. Artículos de revistas científicas


- Colombo P., Ferrari E. 2015. Privacy aware access control for big data: A research roadmap [versión electrónica]. *Big Data Research* 2 (Issue 4): 145 – 154.
- Du Z., Liu Y., Wang Y. 2013. Relation based access control in campus social network System [versión electrónica]. *Procedia Computer Science* 17: 14 – 20.
- Goncalves G., Poniszewska-Maranda A. 2007. Role engineering: From design to evolution of security schemes [versión electrónica]. *The Journal of Systems and Software* 81 (Issue 8): 1306 – 1326.
- Gouglidis A., Mavridis I. 2012. domRBAC: An access control model for moderm collaborative systems [versión electrónica]. *Computers & Security* 31 (Issue 4): 540 – 556.
- Hung Le X., Doll T., Barbosu M., Luque A., Wang D. 2012. An enhancement of the role-based access control model to facilitate information access management in context of team collaboration and workflow [versión electrónica]. *Journal of Biomedical Informatics* 45 (Issue 6): 1084 – 1107.
- Kim S., Kim D., Lu L., Kim S., Park S. 2011. A feature-based approach for modeling role-based access control systems [versión electrónica]. *The Journal of Systems and Software* 84 (Issue 12): 2035 – 2052.
- Lee B., Kim D., Yang H., Jang H. 2015. Role-based access control for substation automation systems using XACML [versión electrónica]. *Information Systems* 53: 237 – 249.
- Smari WW., Clemente P., Lalande JF. 2014. An extended attribute based access control model with trust and privacy: Application to a collaborative crisis management system [versión electrónica]. *Future Generation Computer Systems* 31: 147 – 168.
- Tounis YA., Kifayat K., Merabti M. 2014. An access control model for cloud computing [versión electrónica]. *Journal of Information Security and Application* 19 (Issue 1): 45 – 60.
- Wang H., Guo X., Fan Y., Bi J. 2014. Extended access control and recommendation methods for enterprise knowledge management system [versión electrónica]. *IERI Procedia* 10: 224 – 230.

- Yang-Feng J., Si-Yue Z., Zhen H., Mu-Qing L., Ling Y., Jing-Ping N. 2013. Access control for rural medical and health collaborative working platform [versión electrónica]. *The Journal of Chine Universities of Posts and Telecommunications* 20 (Suppl. 2): 7 – 10.


**2. Libros**


- Aneta Petrova, Tomas Capek, Ella Deon Ballard. 2016. *Red Hat Enterprise Linux 7 Linux Domain Identity, Authentication, and Policy Guide*. EE. UU.: Red Hat, Inc.
- Tomas Capek, Aneta Petrova, Ella Deon Ballard. 2016. *Red Hat Enterprise Linux 7 Windows Integration Guide*. EE. UU.: Red Hat, Inc.
- Julio Téllez Valdés. 2009. *Derecho Informático,* 4ª ed. México: McGranwHill.
- Mark Heslin. 2013. Integrating Red Hat Enterprise Linux 6 with Active Directory. EE. UU.: Red Hat, Inc.
- Thomas R. Peltier. 2014. *Information Security Fundamentals*, 2ª ed. EE. UU: Taylor & Frances Group.


**3. Sitio de Web**


- Portal de la Oficina Nacional de Gobierno Electrónico e Informática ONGEI. 2009. *Norma Técnica Peruana PNTP-ISO/IEC 27001:2008 EDI. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos, 1ª Edición.* [Internet], [02 diciembre 2015]. Disponible en: http://www.ongei.gob.pe
- Portal de la Oficina Nacional de Gobierno Electrónico e Informática ONGEI. 2007. *Norma Técnica Peruana PNTP-ISO/IEC 17799:2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información, 2ª Edición.* [Internet], [02 diciembre 2015]. Disponible en: http://www.ongei.gob.pe
- Portal del Partner Center de Red Hat. 2014. *Datasheet*, *Red Hat Enterprise Linux Server Datasheet.* [Internet], [30 noviembre 2015]. Disponible en: https://partnercenter.force.com
- Portal del Partner Center de Red Hat. 2014. *Informe Tecnológico*, *Red Hat Enterprise Linux: Gestión de identidades* [Internet], [30 noviembre 2015]. Disponible en: https://partnercenter.force.com

- Portal del Partner Center de Red Hat. 2014. *Whitepaper*, *Doing more with less, How Red Hat Enterprise Linux shrinks total cost of ownership (TCO) compared to Windows*. [Internet], [30 de noviembre 2015]. Disponible en: https://partnercenter.force.com

**ANEXOS**

## 1. Instalación del servidor Red Hat Identity Management

Instalar los siguientes paquetes a través de la herramienta *yum*.

```
[ root@server ~ ] # yum  install  ipa-server  bind  bind-dyndb-ldap  -y
```

Ejecutar la herramienta *ipa-server-install* para iniciar la instalación del servidor *Red Hat Identity Management* con funciones de servidor *DNS*.

```
[ root@server ~ ] # ipa-server-install  --setup-dns
```

Escribir *yes* para reiniciar el archivo de configuración del servicio *DNS* que se aloja en el servidor por defecto y presionar la tecla *Enter* para continuar.

**Existing BIND configuration detected, overwrite? [no] :** ***yes***

Escribir el nombre del servidor en formato *FQDN* y presionar la tecla *Enter* para continuar.

**Server host name [ ... ] :** ***hostname.en.fqdn***

Escribir el nombre del dominio y presionar la tecla *Enter* para continuar.

**Please confirm the domain name [ ... ] :** ***nombre.del.dominio***

Escribir el *realm name* para el servicio *Kerberos* y presionar la tecla *Enter* para continuar.

**Please provide a realm name [ ... ] :** ***realname***

Escribir la contraseña para el super usuario del servicio de directorio *Red Hat Identity Management* y presionar la tecla *Enter* para continuar.

**Directory Manager password : *contraseña***
**Password (confirm) : *contraseña***

Escribir la contraseña para la cuenta de usuario *admin* del sistema R*ed Hat Identity Management* y presionar la tecla *Enter* para continuar.

**IP admin password: *contraseña***
**Password (confirm) : *contraseña***

Escribir *no* para no indicar un servidor al cual se le reenviara las consultas del servicio *DNS* y presionar la tecla *Enter* para continuar.

**Do you want to configure DNS forwarders? [yes] : *no***

Escribir *yes* para configurar la *zona reversa* del servicio *DNS*, especificar el nombre de la zona reversa y presionar la tecla *Enter* para continuar.

**Do you want to configure the reverse zone? [yes] : *yes***
**Please specify the reverse zone name [...] : *zonareversa.in-addr.arpa.***

Escribir *yes* para confirmar los parámetros de configuración del sistema y presionar la tecla *Enter* para continuar.

**Continue to configure the system with these values? [no] : *yes***

## 2. Instalación de los clientes de Identity Management

Instalar los siguientes paquetes a través de la herramienta *yum*.

```
[ root@server ~ ] # yum  install  ipa-client  ipa-admintools  -y
```

Ejecutar la herramienta *ipa-client-install* para iniciar la instalación del client de *Red Hat Identity Management.*

```
[ root@server ~ ] # ipa-client-install  --enable-dns-updates
```

Escribir *yes* para confirmar los parámetros de configuración del sistema encontrados en el dominio y presionar la tecla *Enter* para continuar.

```
Continue to configure the system with these values? [no] : yes
```

Escribir la cuenta *admin* y su contraseña parar confirmar el usuario autorizado de enrolamientos de sistemas clientes y presionar la tecla *Enter* para continuar.

```
User authorized to enroll computers : admin
Password for admin@DOMAIN.NAME: password
```

## 3. Instalación del servicio Samba

Instalar los siguientes paquetes a través de la herramienta *yum*.

```
[ root@server ~ ] # yum  install  samba  samba-client  samba-common
samba-winbind  samba-winbind-clients  -y
```